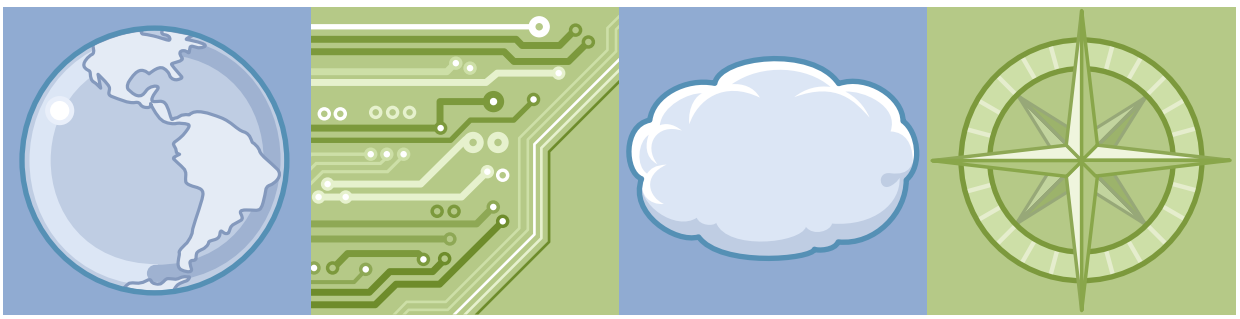
IBM Training

Instructor Guide

InfoSphere Guardium V9 Technical Training

Course code GU202 ERC 2.0



Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	AS/400®	DB™
DB2®	Guardium®	Informix®
InfoSphere®	S-TAP®	System z®
Tivoli®	z/OS®	

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

VMware and the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

Netezza® is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

Other product and service names might be trademarks of IBM or other companies.

September 2013 edition

The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

© Copyright International Business Machines Corporation 2011, 2013.
This document may not be reproduced in whole or in part without the prior written permission of IBM.
US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Trademarks xv

Instructor course overview xvii

Course description xix

Agenda xxi

Unit 1. InfoSphere Guardium 1-1
Unit objectives 1-2
Main features 1-3
The need for database access monitoring 1-4
Native auditing 1-5
Guardium's database access monitoring 1-6
Monitoring at the network level 1-7
Logging example 1-8
Guardium components 1-9
Real-time monitoring (1 of 2) 1-10
Real-time monitoring (2 of 2) 1-11
Built-in and custom reporting 1-12
Compliance Workflow Automation 1-13
Configuration Auditing System 1-14
Vulnerability Assessment 1-15
Database Discovery 1-16
Data Classification 1-17
Checkpoint (1 of 2) 1-18
Checkpoint (2 of 2) 1-20
Unit summary 1-22
Checkpoint solutions (1 of 2) 1-23
Checkpoint solutions (2 of 2) 1-24

Unit 2. Guardium Architecture 2-1
Unit objectives 2-2
2.1. Data collection methods 2-3
Data collection methods 2-4
Collector 2-5
Span port collection method 2-7
Network tap collection method 2-9
STAP: Local monitoring 2-11
STAP: Local and network monitoring 2-12
Raw network traffic 2-14
Topic summary 2-15
2.2. Aggregation, Central Management, and Integration 2-17
Aggregation, central management, and integration 2-18

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Hardware and software 2-19
Collection 2-20
Aggregation 2-21
Central management (1 of 2) 2-22
Central management (2 of 2) 2-23
Small environments 2-24
Medium-sized environments 2-25
Larger-sized environments 2-26
Integration 2-27
Topic summary 2-29
Checkpoint 2-30
Unit summary 2-32
Checkpoint solutions 2-33

Unit 3. Command Line Interface 3-1
Unit objectives 3-2
CLI overview (1 of 2) 3-3
CLI overview (2 of 2) 3-4
CLI users 3-6
CLI password requirements 3-8
CLI user login (1 of 2) 3-10
CLI user login (2 of 2) 3-11
Navigating the CLI (1 of 4) 3-12
Navigating the CLI (2 of 4) 3-14
Navigating the CLI (3 of 4) 3-16
Navigating the CLI (4 of 4) 3-17
Show and store 3-18
Reminder: CLI command categories 3-19
Network configuration commands 3-20
Aggregator commands 3-22
Alerter configuration commands 3-23
Configuration and control commands 3-24
File handling commands 3-25
Diagnostic commands 3-26
Inspection engine commands 3-27
User account, password, and authentication commands 3-28
Generate new layout command 3-29
Certificate commands 3-30
GuardAPI (1 of 2) 3-31
GuardAPI (2 of 2) 3-32
Checkpoint 3-33
Unit summary 3-35
Exercise 3-36
Checkpoint solutions 3-37

Unit 4. Access Management 4-1
Unit objectives 4-2
accessmgr 4-3

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Management GUI panes 4-4
Access Management tab 4-5
User Browser 4-6
User Browser - adding a user (1 of 2) 4-8
User Browser - adding a user (2 of 2) 4-10
User Browser - editing a user 4-11
User Browser - modifying roles 4-12
User Browser - changing layouts 4-13
User Browser - deleting a user 4-14
User Role Browser 4-15
User Role Permissions 4-17
User LDAP Import 4-18
User & Role Reports 4-19
Data Security tab 4-20
Checkpoint (1 of 2) 4-21
Checkpoint (2 of 2) 4-23
Unit summary 4-25
Exercise 4-26
Checkpoint solution (1 of 2) 4-27
Checkpoint solution (2 of 2) 4-28

Unit 5. System View and Administration Console I. 5-1
Unit objectives 5-2
System View 5-3
Administration Console 5-5
Administration Console - Configuration 5-6
Configuration - Alerter 5-7
Configuration - Anomaly Detection 5-9
Configuration - Application User Translation 5-11
Configuration - Custom ID Procedures 5-13
Configuration - Customer Uploads 5-14
Configuration - Flat Log Process 5-16
Configuration - Global Profile 5-18
Configuration - Guardium for z/OS 5-20
Configuration - Incident Generation Process 5-21
Configuration - Inspection Engines (1 of 2) 5-22
Configuration - Inspection Engines (2 of 2) 5-24
Configuration - IP-to-Hostname Aliasing 5-25
Configuration - Policy Installation 5-27
Configuration - Portal 5-28
Configuration - Query Hint 5-29
Configuration - Session Inference 5-30
Configuration - System 5-31
Configuration - Upload Key File 5-33
Checkpoint 5-34
Unit summary 5-36
Checkpoint solutions 5-37

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 6. System View and Administration Console II 6-1
Unit objectives 6-2
Administration Console - Data Management 6-3
Data Management - Data archive and purge 6-4
Data Management - Data Export 6-6
Data Management - Data Import (Aggregator only) 6-7
Data Management - Data Restore 6-8
Data Management - Catalog Archive 6-9
Data Management - Catalog Export 6-10
Data Management - Catalog Import 6-11
Data Management - Results Archive (audit) 6-12
Data Management - Results Export (files) 6-13
Administration Console - Central Management 6-14
Registering to a CM from a collector 6-15
Registering a unit from the Central Manager 6-16
Standalone versus Managed By 6-17
Central Management screen 6-18
Portal User Sync 6-20
Local Taps 6-21
Export definitions 6-22
Import definitions 6-23
Distributed Interface 6-24
Custom Alerting 6-25
Module Installation 6-26
Checkpoint (1 of 2) 6-27
Checkpoint (2 of 2) 6-29
Unit summary 6-31
Exercise 6-32
Checkpoint solution (1 of 2) 6-33
Checkpoint solution (2 of 2) 6-34

Unit 7. S-TAP and GIM 7-1
Unit objectives 7-2
S-TAP overview 7-3
S-TAP installation methods 7-4
S-TAP ports 7-5
Installation resources 7-6
7.1. Interactive installation: Windows 7-7
Interactive installation: Windows 7-8
Windows STAP interactive installation: setup.exe 7-9
Setup type: Custom 7-10
Choose Destination Location 7-11
Select Features 7-12
Copy Files 7-13
S-TAP host 7-14
Collector IP address 7-15
Additional collector for failover 7-16
Start S-TAP service 7-17

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Complete installation 7-18
Confirm services 7-19
S-TAP Control status 7-20
S-TAP Configuration: Details (1 of 2) 7-21
S-TAP Configuration: Details (2 of 2) 7-23
S-TAP Configuration: CAS and Application Server User ID 7-25
S-TAP Configuration: Guardium Hosts 7-26
Add Inspection Engines 7-28
Confirm Inspection Engine 7-30
Verify traffic 7-31
Topic summary 7-32
7.2. GIM installation: UNIX/Linux 7-33
GIM installation: UNIX/Linux 7-34
GIM overview 7-35
Download and extract GIM installer 7-36
GIM installers directory 7-37
Installing GIM 7-38
Confirm installation from the GUI 7-40
Module Upload 7-41
Setup By Client 7-42
Select clients 7-43
Common modules 7-44
Module Parameters 7-45
Client Module Parameters (1 of 2) 7-46
Client Module Parameters (2 of 2) 7-47
Schedule installation 7-48
GIM Events List 7-49
Discovery Setup By Module 7-50
Bundle-discovery 7-51
Select client 7-52
Java installation directory 7-53
Schedule installation 7-54
GIM Events List 7-55
Create S-TAP inspection engine 7-56
Invoke now 7-57
Complete process 7-58
Confirm Inspection Engine creation 7-59
Verify traffic 7-60
Topic summary 7-61
7.3. S-TAP installation: Non-interactive methods 7-63
S-TAP installation: Non-interactive methods 7-64
UNIX non-interactive installer 7-65
Windows non-interactive installer 7-67
GrdApi inspection engine creation 7-69
Topic summary 7-71
Checkpoint 7-72
Unit summary 7-74
Exercise 7-75

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution 7-76
Checkpoint solution continued 7-77

Unit 8. Group Builder 8-1
Unit objectives 8-2
Group: Definition 8-3
Methods to build groups 8-5
Accessing Group Builder 8-6
Group Builder screen overview 8-7
Modify existing groups (1 of 2) 8-8
Modify existing groups (2 of 2) 8-9
Create New Group 8-10
Manual entry (1 of 2) 8-12
Manual entry (2 of 2) 8-13
Auto Generated Calling Prox (1 of 2) 8-14
Auto Generated Calling Prox (2 of 2) 8-16
Auto Generated Calling Prox: Options 8-17
Auto Generated Calling Prox: Using DB sources 8-19
Auto Generated Calling Prox example (1 of 6) 8-20
Auto Generated Calling Prox example (2 of 6) 8-21
Auto Generated Calling Prox example (3 of 6) 8-22
Auto Generated Calling Prox example (4 of 6) 8-23
Auto Generated Calling Prox example (5 of 6) 8-24
Auto Generated Calling Prox example (6 of 6) 8-25
LDAP (1 of 2) 8-26
LDAP (2 of 2) 8-27
Populate from Query (1 of 4) 8-28
Populate from Query (2 of 4) 8-29
Populate from Query (3 of 4) 8-31
Populate from Query (4 of 4) 8-32
Classifier 8-33
GuardAPI (1 of 2) 8-34
GuardApi (2 of 2) 8-35
Hierarchical groups (1 of 3) 8-36
Hierarchical groups (2 of 3) 8-37
Hierarchical groups (3 of 3) 8-38
Group reports 8-39
Checkpoint (1 of 2) 8-40
Checkpoint (2 of 2) 8-42
Unit summary 8-44
Exercise 8-45
Checkpoint solution (1 of 2) 8-46
Checkpoint solution (1 of 2 continued) 8-47
Checkpoint solution (2 of 2) 8-48

Unit 9. . . . . Policies 9-1
Unit objectives 9-2
9.1. Policy overview 9-3

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Policy overview . . . 9-4
Policies defined . . . 9-5
Default behavior: Traffic . . . 9-6
Default behavior: Parsing and logging . . . 9-8
Constructs (1 of 2) . . . 9-10
Constructs (2 of 2) . . . 9-12
Checkpoint . . . 9-14
Topic summary . . . 9-16
Checkpoint solutions . . . 9-17
9.2. Installing and creating policies. . . . 9-19
Installing and creating policies . . . 9-20
Install policy . . . 9-21
Currently Installed Policies . . . 9-23
Accessing the Policy Builder . . . 9-24
Create a new policy . . . 9-25
Policy Definition (1 of 2) . . . 9-27
Policy Definition (2 of 2) . . . 9-29
Policy Rules . . . 9-30
Checkpoint . . . 9-31
Topic summary . . . 9-33
Checkpoint solutions . . . 9-34
Exercise . . . 9-35
9.3. Access Rules. . . . 9-37
Access rules . . . 9-38
Access Rule: Overview . . . 9-39
Access Rule: Description . . . 9-40
Access Rule: Criteria . . . 9-41
Access Rule: Action and Back/Save . . . 9-42
Access Rule: Actions . . . 9-43
Access Rule: Example . . . 9-45
Alert rules . . . 9-46
Alert example . . . 9-48
Policy violation . . . 9-49
Allow . . . 9-50
Ignore session rules . . . 9-52
Ignore STAP session . . . 9-53
Ignore STAP Session rule . . . 9-55
Ignore sessions and sizing . . . 9-56
Ignore STAP session rule: Trusted connections . . . 9-57
Trusted connections group . . . 9-58
Ignore session criteria . . . 9-59
Ignore STAP session example . . . 9-60
Ignore responses per session . . . 9-61
Ignore SQL per session . . . 9-62
Ignore session . . . 9-63
Session ignored values . . . 9-64
Log full details . . . 9-65
Log full details: Example . . . 9-66

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log full details per session 9-67
Log masked details 9-68
Log only 9-69
Quick parse 9-70
Skip logging 9-71
Checkpoint 9-72
Topic summary 9-74
Checkpoint solutions 9-75
9.4. Exception and Extrusion Rules 9-77
Exception and Extrusion rules 9-78
Exception Rule overview 9-79
Exception Rule Definition 9-80
Failed login alert 9-81
Extrusion Rules 9-82
Extrusion Rule example 9-83
Extrusion rule results example 9-85
Checkpoint 9-86
Topic summary 9-88
Checkpoint solutions 9-89
Checkpoint solutions continued 9-90
9.5. Selective Audit Trail policy 9-91
Selective Audit Trail policy 9-92
Creating a Selective Audit Trail policy 9-93
Selective Audit Trail default behavior 9-94
Audit Only rule 9-96
Checkpoint 9-97
Topic summary 9-99
Checkpoint solution 9-100
9.6. Rule Order and Logic 9-101
Rule order and logic 9-102
Rule order and policy logic 9-103
Policy logic 9-105
Checkpoint 9-107
Topic summary 9-109
Checkpoint solutions 9-110
Exercise 9-111
9.7. S-GATE 9-113
S-GATE 9-114
S-GATE overview 9-115
S-GATE S-TAP settings 9-116
S-GATE ATTACH/DETACH 9-118
S-GATE Terminate 9-119
Redact 9-120
Quarantine 9-121
Topic summary 9-122
Checkpoint 9-123
Unit summary 9-125
Exercise 9-126

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions 9-127

Unit 10. CAS, VA, and Discovery 10-1
Unit objectives 10-2
CAS 10-3
CAS Components 10-4
Configuration Auditing System (1 of 3) 10-6
Configuration Auditing System (2 of 3) 10-8
Configuration Auditing System (3 of 3) 10-10
VA 10-12
Vulnerability Assessment (1 of 4) 10-13
Vulnerability Assessment (2 of 4) 10-14
Vulnerability Assessment (3 of 4) 10-15
Vulnerability Assessment (4 of 4) 10-18
Database Discovery and classification (1 of 2) 10-19
Database Discovery and classification (2 of 2) 10-20
Checkpoint (1 of 2) 10-21
Checkpoint (2 of 2) 10-23
Unit summary 10-25
Exercise 10-26
Checkpoint solutions (1 of 2) 10-27
Checkpoint solutions (2 of 2) 10-28

Unit 11. Custom Query and Report Building 11-1
Unit objectives 11-2
11.1. Query overview and creating a simple query 11-3
Query overview and creating a simple query 11-4
Creating a custom query 11-5
Track data access 11-6
Domain 11-7
Query finder: New query 11-8
New query: Name and main entity 11-9
Main entity: About entities 11-10
Access domain entities 11-11
Logging and parsing 11-13
Entity Hierarchy 11-14
Main entity: Effects 11-15
New query steps summary 11-16
Custom query builder 11-17
Adding fields 11-18
Changing query settings 11-20
Adding a condition, saving and publishing report 11-22
Viewing a report 11-23
Customize screen 11-24
Pane buttons 11-26
Report buttons 11-27
Checkpoint 11-29
Topic summary 11-31

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions 11-32
Exercise 11-33
11.2. Query conditions 11-35
Query conditions 11-36
New query: Object main entity 11-37
Query conditions (1 of 2) 11-38
Query conditions (2 of 2) 11-40
Addition mode: AND/OR 11-42
Having 11-43
Parenthesis 11-44
Run Time Parameters / Dynamic groups 11-45
Run Time Parameters / Dynamic groups: Results 11-46
Drill-down reports 11-47
Drill-down report example 11-48
Special drill-down options 11-49
Query buttons 11-50
Topic summary 11-52
Checkpoint (1 of 2) 11-53
Checkpoint (2 of 2) 11-55
Exercise 11-57
Checkpoint solutions (1 of 2) 11-58
Checkpoint solutions (2 of 2) 11-59
11.3. Report Builder 11-61
Report builder 11-62
Report builder 11-63
Searching for a report 11-64
Report builder buttons 11-65
Modify report: Tabular (1 of 2) 11-67
Modify report: Tabular (2 of 2) 11-68
Modify report: Chart (1 of 2) 11-69
Modify report: Chart (2 of 2) 11-70
Topic summary 11-71
Checkpoint 11-72
Unit summary 11-74
Exercise 11-75
Checkpoint solutions 11-76

Unit 12. Compliance Workflow Automation 12-1
Unit objectives 12-2
Compliance Workflow Automation 12-3
Compliance Workflow Automation elements 12-4
Compliance Workflow Automation log 12-6
Define an Audit Process 12-7
Compliance Automation screen 12-8
Audit Process Definition 12-9
Receiver Table 12-11
Audit Tasks 12-13
Roles/Process Management 12-15

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Activating and running an audit process 12-16
To Do notification 12-17
Viewing an audit process 12-18
Report delivery 12-19
Workflow results 12-20
Checkpoint 12-21
Unit summary 12-23
Exercise 12-24
Checkpoint solutions 12-25

Appendix A. Monitoring Overview A-1
A.1. Introduction A-1
A.2. Intended Audience A-1
A.3. Gathering Requirements A-1
A.4. Building Groups A-2
A.5. Defining Policy A-4
A.6. Creating Reports A-7
A.7. Adding Guardium Users and Roles A-12
A.8. Developing Workflow A-14
A.9. Appendix A-16

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	AS/400®	DB™
DB2®	Guardium®	Informix®
InfoSphere®	S-TAP®	System z®
Tivoli®	z/OS®	

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

VMware and the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

Netezza® is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

Other product and service names might be trademarks of IBM or other companies.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor course overview

This course enables the students to acquire the skills necessary to create reports, audits, alerts, metrics, compliance oversight processes, and database access policies and controls.

This course also teaches the students how to archive, purge and backup.

Course strategy

Teaching strategy

Each classroom session uses a combination of facilitated lecture, discussions, group exercises, and demonstrations to convey the material.

Introduce the material

Inform the students of the objectives of the unit and topic. Give them a brief scenario that helps them understand how the presented material helps them do their jobs.

Facilitate the learning experience

Involve the students in the learning process. Ask them questions and present classroom scenarios in which students use the available resources to solve situations that involve process, procedure, or content on the job.

Review the material

Review objectives at the conclusion of each unit to ensure that the students have a thorough understanding of the material.

Group exercises and labs are used to reinforce knowledge and skills that the students learned in the previous classroom topics. The instructor serves as a mentor in checking results, answering questions, and providing constructive feedback and evaluation.

Course evaluation

Evaluation measures the quality, effectiveness, and impact of the course. It enables students to answer the question, "Does the course meet its requirements and objectives?"

For all classes, students will provide feedback on course quality by completing an end-of-course questionnaire.

Measurement plan

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

No formal tests are administered in the class.

Course materials

- *Student Notebook*
- *Instructor Guide*
- PowerPoint visuals in PDF form
- *Student Exercises*
- *Instructor Exercises Guide*

Summary of changes in this edition

The updates in this version of the course are designed to introduce Guardium v9, and to improve the readability of the materials and the instructions for the exercises.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Course description

InfoSphere Guardium V9 Technical Training

Duration: 3 days

Purpose

This three-day course offers a balanced mix of lectures, hands-on lab work, case studies, and testing. Students will learn how to create reports, audits, alerts, metrics, compliance oversight processes, and database access policies and controls. Students will also learn about system administration, archiving, purging, and back-ups.

Audience

This course is for Information Security professionals, Database Administrators, Auditors.

Prerequisites

There are no prerequisites for this course.

Objectives

After completing this course, you should be able to:

- Identify the methods that Guardium uses to capture database traffic
- Navigate the CLI
- Update the network configuration on an appliance
- Understand S-TAP and how to install it
- Create a policy or set of policies to meet your requirements
- Install and manage policies
- Understand the major components of the Configuration Auditing System (CAS)
- Explain how to create custom queries and reports
- Understand how to consolidate and automate audit activities into a compliance workflow

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Agenda

Day 1

(00:30) Welcome
(00:30) Unit 1 - InfoSphere Guardium
(00:30) Unit 2 - Guardium Architecture
(00:30) Unit 3 - CLI - Command Line Interface
(00:15) Exercise 1 - Using the Guardium CLI
(00:30) Unit 4 - Access Management
(00:15) Exercise 2 - Creating Guardium Users
(00:45) Unit 5 - System View and Administration Console I
(00:45) Unit 6 - System View and Administration Console II
(00:30) Exercise 3 Archiving Collected Data
(01:30) Unit 7 - S-TAP and GIM
(00:45) Exercise 4 Installing GIM and S-TAP

Day 2

(01:15) Unit 8 - Group Builder
(00:30) Exercise 5 - Creating Guardium Groups
(01:15) Unit 9 - Policies
(00:45) Exercise 6 - Creating a Policy
(01:15) Unit 9 - Policies
(00:30) Exercise 7 - Updating a Policy
(00:30) Unit 10 - CAS, VA, and Discovery
(00:30) Exercise 8 - Installing and Configuring CAS
(00:30) Exercise 9 - Running a Vulnerability Assessment

Day 3

(01:45) Unit 11 - Custom Query and Report Building
(00:45) Exercise 10 - Creating a Simple Query and Report
(00:45) Exercise 11 - Creating a Query with Drill-down
(00:45) Exercise 12 - Creating Multiple Queries
(01:00) Unit 12 - Compliance Workflow Automation
(01:00) Exercise 13 - Creating a Compliance Workflow

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 1. InfoSphere Guardium

Estimated time

00:30

What this unit is about

This unit gives an introduction to IBM InfoSphere Guardium.

What you should be able to do

After completing this unit, you should be able to:

- Identify the main functionality InfoSphere Guardium
- Describe the key components of the InfoSphere Guardium solution

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Identify the main functionality InfoSphere Guardium
- Describe the key components of the InfoSphere Guardium solution

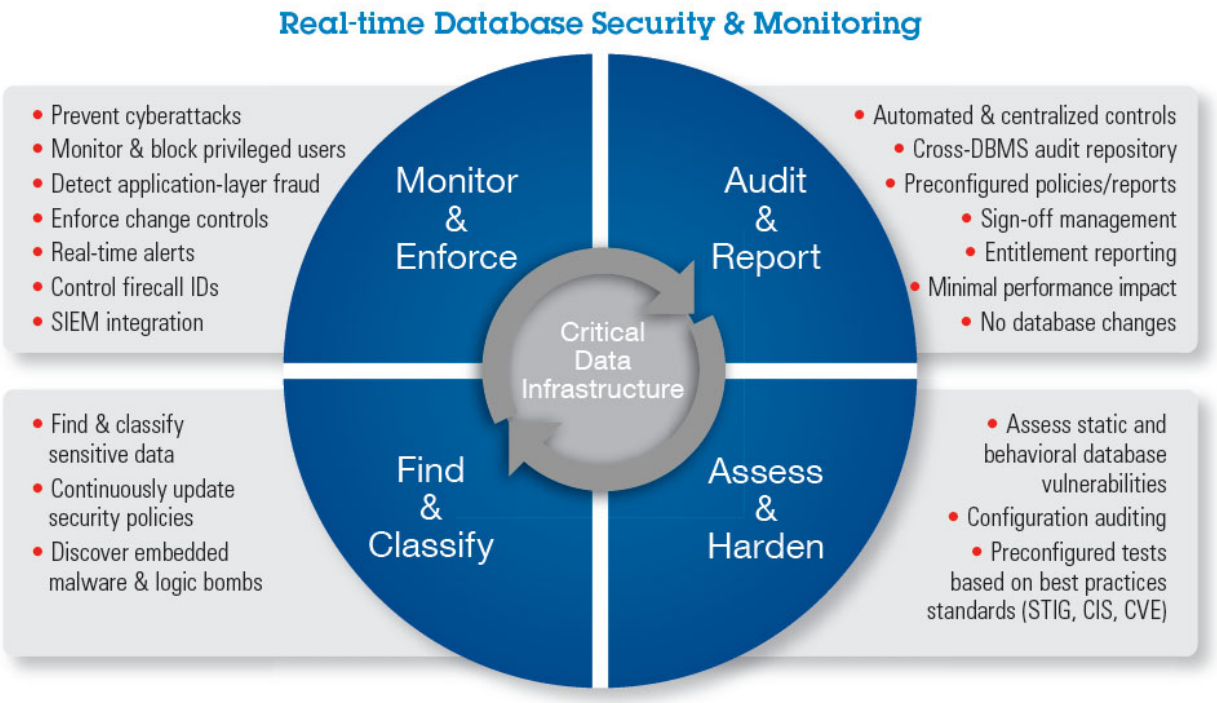
© Copyright IBM Corporation 2011, 2013

Figure 1-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Main features



© Copyright IBM Corporation 2011, 2013

Figure 1-2. Main features GU2022.0

Notes:

IBM InfoSphere Guardium is a database security and monitoring solution that addresses all aspects of database protection, including:

- Database Access Monitoring
- Real-Time Monitoring -- Alerting, Filtering and Prevention through policies and rules
- Reporting – Built-in and Custom
- Compliance Workflow Automation
- Configuration Auditing
- Vulnerability Assessment
- Database Discovery and Data Classification

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The need for database access monitoring

- Regulations and industry standards:
  - SOX – Sarbanes Oxley
  - PCI – Payment Card Industry
  - HIPAA - Health Insurance Portability and Accountability Act
  - and so on

– Many corporations are required to monitor activity performed against their databases:
  - PCI requires that all access to credit card information is logged
  - SOX requires that all privileged user activity is monitored

– Other corporations choose the monitor database activity:
  - To meet their own internal security requirements
  - To protect sensitive and valuable data

© Copyright IBM Corporation 2011, 2013

Figure 1-3. The need for database access monitoring GU2022.0

Notes:

Every company has its own reasons for monitoring database access. It some cases, monitoring is required by industry standards or regulations. In other cases, monitoring is needed to conform to local business rules.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Native auditing

- Without a solution like Guardium, companies must rely on built-in auditing methods (also known as native auditing) within each of their database platforms to meet monitoring requirements
  - Native database auditing is not appropriate in many organizations for a number of reasons, including:
    - High resource utilization
      - Native auditing often consumes 10 to 12% of a server's CPU
    - No separation of duties
      - Because native auditing must be configured from within the database, DBAs have the ability to turn it off and manipulate the log files
      - These same DBAs and other privileged users often require the highest levels of monitoring because they have open access to the database
    - Inconsistent auditing features
      - Each DBMS has a different method of logging and reporting on database activity, making unified reporting difficult if not impossible

© Copyright IBM Corporation 2011, 2013

Figure 1-4. Native auditing GU2022.0

Notes:

Guardium is the ideal solution to the database monitoring needs of companies. However, many companies try to do the monitoring using the native auditing capabilities of the database management systems they work with. There are many drawbacks to native monitoring, including the impact on the database system, the ability of "super users" to bypass native monitoring, and the difficulties of integrating the native monitoring features of multiple database environments.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Guardium's database access monitoring

- IBM InfoSphere Guardium provides a complete monitoring solution that, in most cases, provides greater detail than native auditing methods while addressing their deficiencies:
  - Minimal resource utilization (3 to 5% CPU utilization)
  - DBAs have no access to Guardium, unless provided by a Guardium administrator
  - Guardium collects database traffic from heterogeneous environments and standardizes it, allowing one system to monitor multiple database types.

© Copyright IBM Corporation 2011, 2013

Figure 1-5. Guardium's database access monitoring GU2022.0

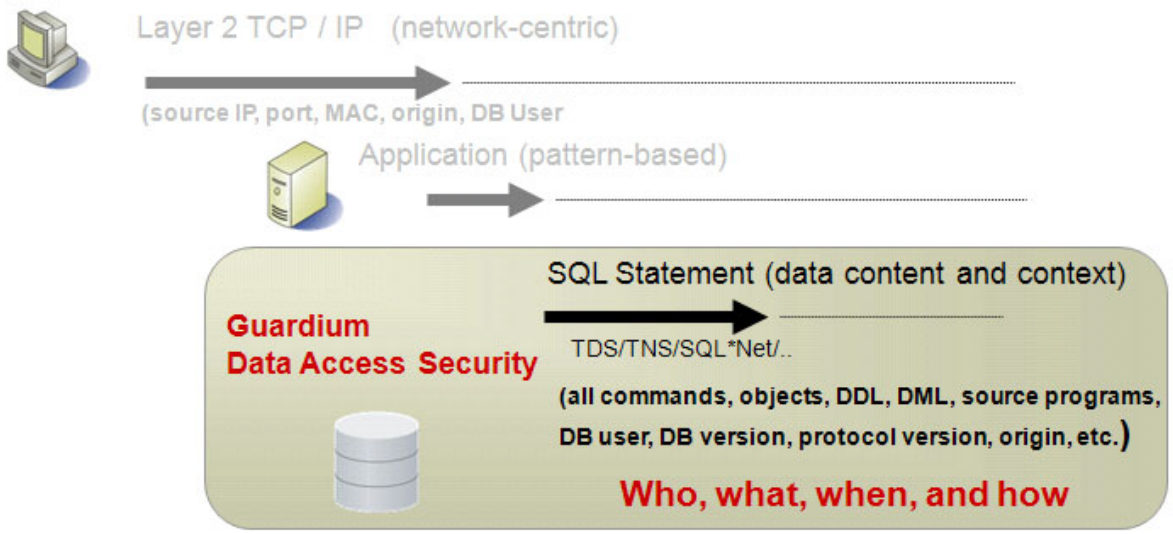
Notes:

IBM InfoSphere Guardium provides a complete solution to a company's monitoring needs. It has minimum impact on the database system operations, is implemented outside the database environment, and works consistently in heterogeneous database environments.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Monitoring at the network level


Layer 2 TCP / IP (network-centric)
(source IP, port, MAC, origin, DB User
Application (pattern-based)
SQL Statement (data content and context)
Guardium
Data Access Security
TDS/TNS/SQL*Net/..
(all commands, objects, DDL, DML, source programs,
DB user, DB version, protocol version, origin, etc.)
Who, what, when, and how

© Copyright IBM Corporation 2011, 2013

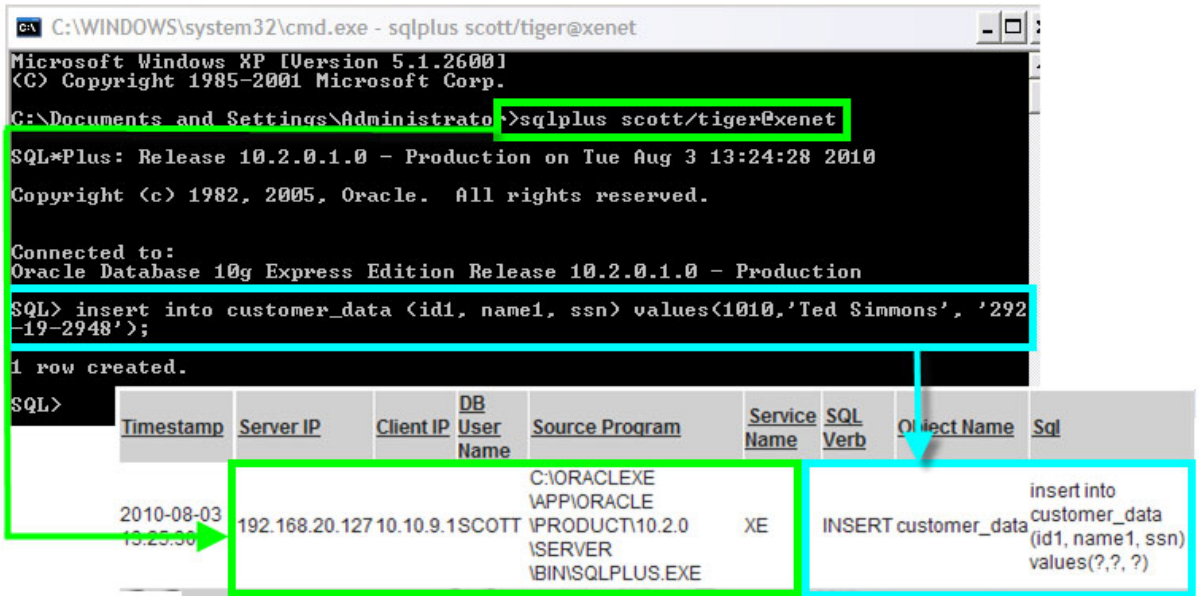
Figure 1-6. Monitoring at the network level GU2022.0

Notes:

Guardium collects traffic at the network level and off-loads the processing to a network appliance. This greatly reduces the resource utilization at the database level, and minimizes any impact on the normal database operations. Guardium's agent (STAP) simply forwards network packets to a network appliance for processing.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Logging example



© Copyright IBM Corporation 2011, 2013

Figure 1-7. Logging example GU2022.0

Notes:

All defined and monitored database activity is logged into Guardium's database in real-time. When a user issues a command or statement against a monitored database, it is immediately logged into Guardium's database and is immediately available for alerting or reporting. Additionally, the strings are parsed into smaller data elements, so that data is easier to categorize and build reports on.

In the example above, the connection 'sqlplus scott/tiger@xenet' is broken down to the database user name, source program, and service name. The client IP and server IP are automatically logged along with this connection information.

In addition to the entire SQL request being logged, it is also broken down into its constituent parts; the SQL Verb (INSERT) and object name (customer_data).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Guardium components

Guardium components include:

- Real-time monitoring
- Built-in and custom reporting
- Compliance Workflow Automation
- Configuration Auditing System
- Vulnerability Assessment
- Database Discovery and Data Classification

© Copyright IBM Corporation 2011, 2013

Figure 1-8. Guardium components GU2022.0

Notes:

Guardium consists of several components – some of them built-in to the product, and some of them add-on. The base product includes components for doing real-time database access monitoring (including options to filter what is being monitored, to generate an alert whenever specific access is attempted, and to terminate access when needed), reporting (both built-in and customized), and compliance workflow (which automatically routes reports to the appropriate users). Additional add-on components provide configuration auditing (to monitor access and changes to supporting database objects), vulnerability assessment (to locate and classify potential areas of risk), and database discovery and data classification (to automatically detect database existence and locate data artifacts).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Real-time monitoring (1 of 2)

Guardium uses **rules** and **policies** to perform real-time filtering, alerting, and prevention:

- Rule – A set of filtering criteria and actions
- Policy – A set of rules to be enforced
- Filtering – Criteria specifying what is to be monitored
- Alerting – Notification when specific actions occur
- Prevention – Blocking actions before they are processed

© Copyright IBM Corporation 2011, 2013

Figure 1-9. Real-time monitoring (1 of 2) GU2022.0

Notes:

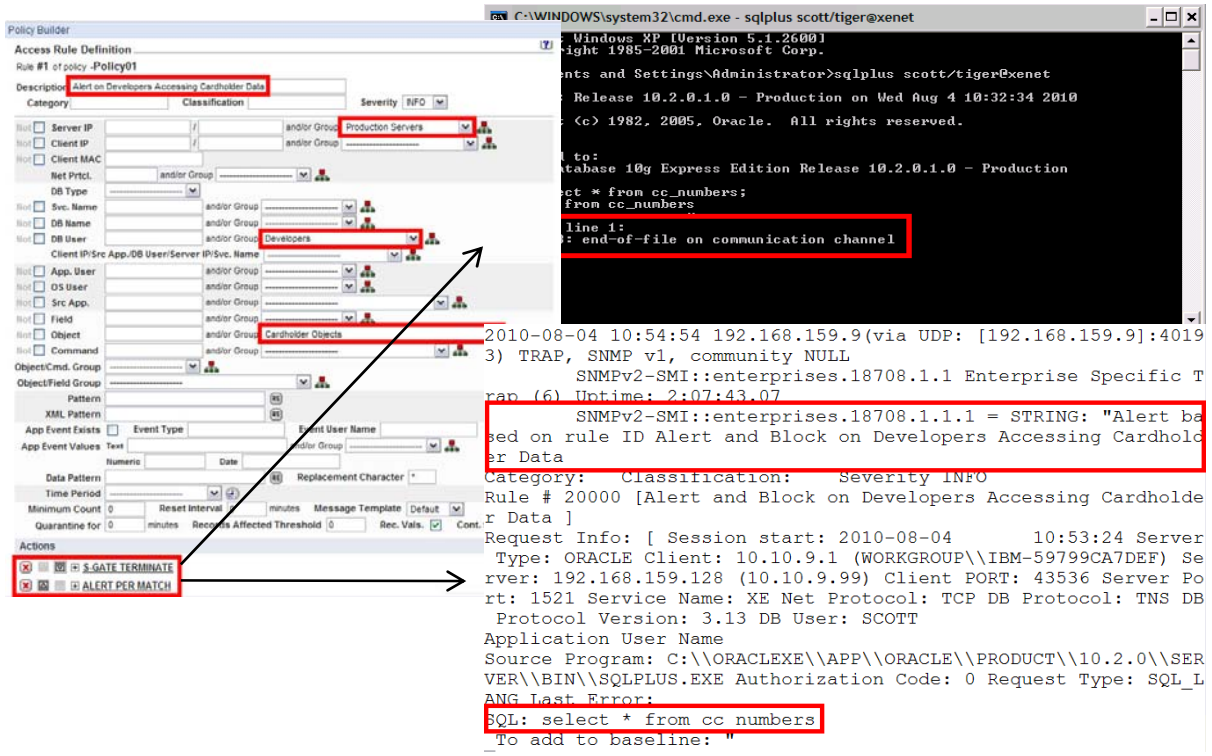
Guardium does not simply log database activity; using policies and rules defined by the Guardium administrators, it can automatically perform specific actions (blocking, alerting, etc.) in real time.

A policy is set of rules applied against the database traffic as it is being monitored and logged into the Guardium appliance database. Each rule contains a set of criteria and one or more actions.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Real-time monitoring (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 1-10. Real-time monitoring (2 of 2) GU2022.0

Notes:

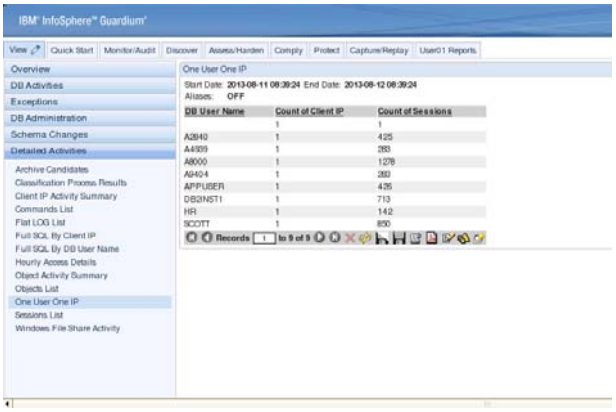
In this example, Guardium will block anyone in the developer group from accessing cardholder objects on production servers. It will also terminate the user's connection and send an alert to the Guardium administrators via SNMP.

As a result of the rule being triggered:

- The command does not reach the database server
- The user's session is terminated
- An alert is sent via SNMP

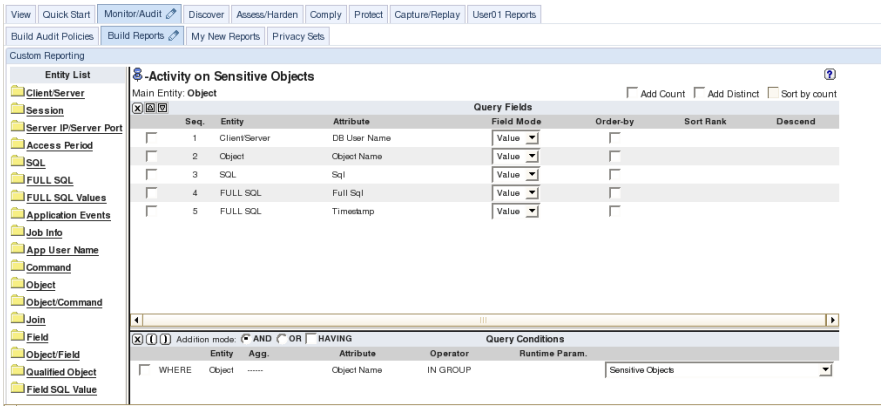
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Built-in and custom reporting



Built-in Reports

Query Builder for Custom Reports



© Copyright IBM Corporation 2011, 2013

Figure 1-11. Built-in and custom reporting GU2022.0

Notes:

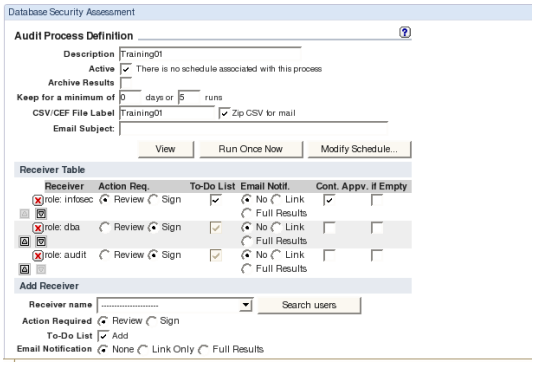
Once the database traffic has been logged into the Guardium appliance database, users can access over 80 pre-built reports for an overview of the database activity. The Guardium solution also includes a flexible query builder, allowing users to create custom reports that meet their specific needs.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Compliance Workflow Automation

Compliance Workflow Automation provides options to:

- Deliver reports, vulnerability assessments, and classification results to the appropriate users on a periodic basis
- Track users who have viewed the reports, signed off on the processes, or added comments



© Copyright IBM Corporation 2011, 2013

Figure 1-12. Compliance Workflow Automation GU2022.0

Notes:

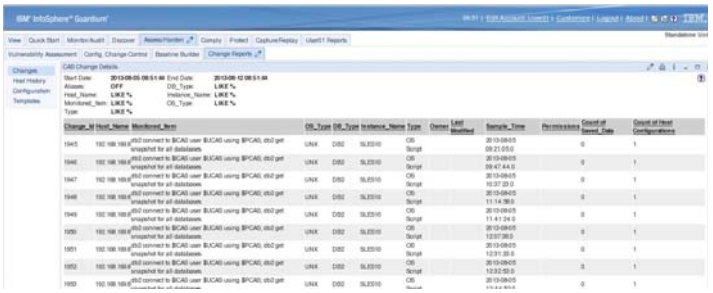
The Guardium solution also includes Compliance Workflow Automation. This feature can be configured to deliver reports, vulnerability assessments, and classification results to the appropriate end users on a periodic basis. This process also tracks who has viewed or signed any process, and also maintains a trail of any comments made by reviewers.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration Auditing System

CAS tracks changes to:

- Security and access control objects
- Database structures
- Critical data values
- Database configuration files
- And so on



© Copyright IBM Corporation 2011, 2013

Figure 1-13. Configuration Auditing System GU2022.0

Notes:

Not all database-related activity can be tracked using Database Access Monitoring. For example, changes to database configuration files, like the listener.ora file in Oracle, are made at the operating system level. Guardium's Configuration Auditing System (CAS) monitors changes to these OS database files, as well as changes to environmental variables and actual values with in the database itself.

With Guardium's CAS, organizations can track all changes to:

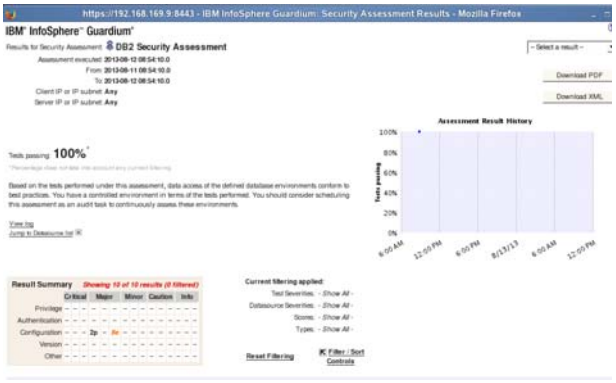
- **Security and access control objects** such as users, roles, and permissions
- **Database structures** such as tables, triggers, and stored procedures. CAS can also detect accidental deletions or insertions of critical tables that can impact data governance.
- **Critical data values** such as data that affects the integrity of financial transactions.
- **Database configuration objects** that can affect security posture such as OS and database configuration files (e.g., sqlnet.ora), environment/registry variables and executables such as shell scripts, Java and XML programs.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Vulnerability Assessment

- VA evaluates the security of the database environment:
  - Query based tests
    - Patches, passwords, privileges, defaults
  - Behavioral tests
    - Exceeding thresholds, executing administrative commands
  - CAS-based tests
    - Operating system configuration vulnerabilities



© Copyright IBM Corporation 2011, 2013

Figure 1-14. Vulnerability Assessment GU2022.0

Notes:

Guardium's Vulnerability Assessment tool evaluates the security of your database environment. It uses three different kinds of tests: query-based tests, behavioral tests, and CAS-based tests.

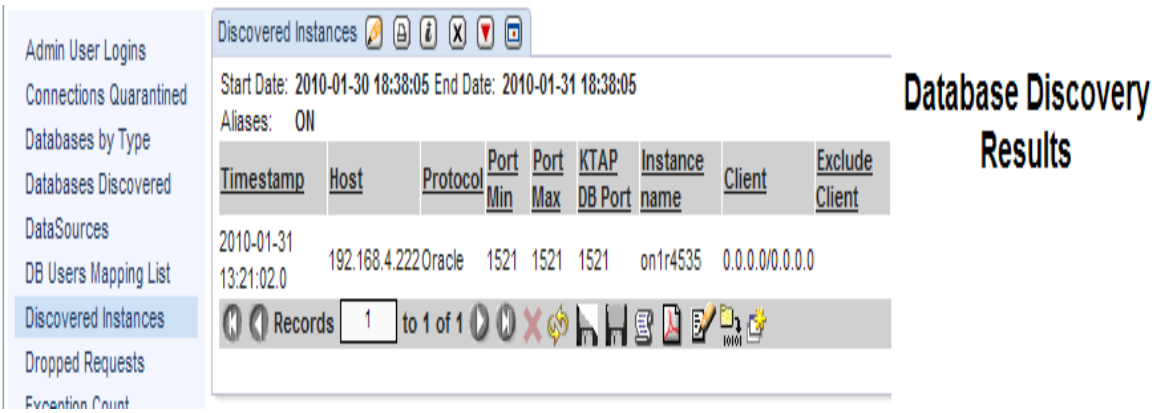
- **Query-based tests** check for vulnerabilities such as missing patches, weak passwords, poorly configured privileges, and default accounts.
- **Behavioral tests** are based on data gathered by Data Access Monitoring and look for items like excessive failed logins, clients executing administrative commands, and after-hours logins.
- **CAS-based tests** look for OS-level configuration vulnerabilities.

After running the selected tests, Guardium presents an overall report card along with details on each result, including recommendations on resolving any issues it identifies as problem areas.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Database Discovery

- Database Discovery
  - Probes the network
  - Locates servers running database services
  - Reports on its findings



© Copyright IBM Corporation 2011, 2013

Figure 1-15. Database Discovery GU2022.0

Notes:

Due to the complexity of some environments and other factors, such as mergers and acquisitions, some companies do not have a full inventory of their database servers. Database Discovery probes a network to identify servers running database services. In the example shown above, Database discovery located a previously unregistered Oracle database server.

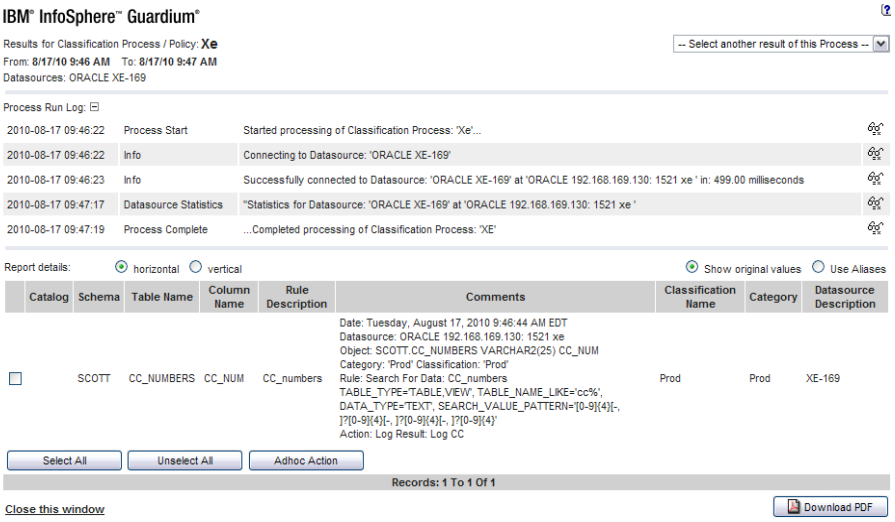
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Classification

- Data Classification
  - Scans databases
  - Locates objects matching certain patterns
  - Reports on its findings

Data Classification Results


IBM® InfoSphere™ Guardium®
Results for Classification Process / Policy: Xe
From: 8/17/10 9:46 AM To: 8/17/10 9:47 AM
Datasources: ORACLE XE-169
-- Select another result of this Process --
Process Run Log:
2010-08-17 09:46:22 Process Start Started processing of Classification Process: 'Xe'...
2010-08-17 09:46:22 Info Connecting to Datasource: 'ORACLE XE-169'
2010-08-17 09:46:23 Info Successfully connected to Datasource: 'ORACLE XE-169' at 'ORACLE 192.168.169.130: 1521 xe ' in: 499.00 milliseconds
2010-08-17 09:47:17 Datasource Statistics "Statistics for Datasource: 'ORACLE XE-169' at 'ORACLE 192.168.169.130: 1521 xe '
2010-08-17 09:47:19 Process Complete ...Completed processing of Classification Process: 'XE'
Report details: horizontal vertical
Show original values Use Aliases
Catalog Schema Table Name Column Name Rule Description Comments Classification Name Category Datasource Description
SCOTT CC_NUMBERS CC_NUM CC_numbers
Date: Tuesday, August 17, 2010 9:46:44 AM EDT
Datasource: ORACLE 192.168.169.130: 1521 xe
Object: SCOTT.CC_NUMBERS VARCHAR2(25) CC_NUM
Category: 'Prod' Classification: 'Prod'
Rule: Search For Data: CC_numbers
TABLE_TYPE='TABLE,VIEW', TABLE_NAME_LIKE='cc%',
DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='[0-9]{4}[-,
]?[0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}'
Action: Log Result: Log CC
Prod Prod XE-169
Select All
Unselect All
Adhoc Action
Records: 1 To 1 Of 1
Close this window
Download PDF

© Copyright IBM Corporation 2011, 2013

Figure 1-16. Data Classification GU2022.0

Notes:

Additionally, also due to the complexity of some environments and other factors, such as mergers and acquisitions, some companies do not know where all of their sensitive data resides. Data Classification scans databases to find and classify any objects or fields containing sensitive data. In the example shown above, Data Classification has located a column in a table which might contain sensitive credit card data.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. List three drawbacks to doing native auditing rather than using a product like Guardium.

2. What is a rule and what is a policy?

© Copyright IBM Corporation 2011, 2013

Figure 1-17. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

1. List three drawbacks to doing native auditing rather than using a product like Guardium.

   High resource utilization - significant impact on the database environment

   No separation of duties - ability of “super users” to bypass native auditing

   Inconsistent auditing features - difficulty of integrating auditing features of multiple database systems

2. What is a rule and what is a policy?

   A rule is a set of filtering criteria and actions.

   A policy is a set of rules to be enforced.

Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (2 of 2)

3. Match the following Guardium components with their correct usage:

a) Real time monitoring	___	Tracks changes to database setup files and security objects
b) Reporting	___	Locates operating databases
c) Compliance Workflow Automation	___	Performs database access filtering, alerting, and prevention
d) Configuration Auditing System	___	Locates sensitive data
e) Vulnerability Assessment	___	Generates built-in or custom documents
f) Database Discovery	___	Tests to evaluate the overall security of the database environment
g) Data Classification	___	Routes reports to users for comments and sign-off

© Copyright IBM Corporation 2011, 2013

Figure 1-18. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

3,

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Match the following Guardium components with their correct usage:

a Real time monitoring	**d** Tracks changes to database setup files and security objects
b Reporting	**f** Locates operating databases
c Compliance Workflow Automation	**a** Performs database access filtering, alerting, and prevention
d Configuration Auditing System	**g** Locates sensitive data
e Vulnerability Assessment	**b** Generates built-in or custom documents
f Database Discovery	**e** Tests to evaluate the overall security of the database environment
g Data Classification	**c** Routes reports to users for comments and sign-off

Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Identify the main functionality InfoSphere Guardium
- Describe the key components of the InfoSphere Guardium solution

© Copyright IBM Corporation 2011, 2013

Figure 1-19. Unit summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (1 of 2)

1. List three drawbacks to doing native auditing rather than using a product like Guardium.

   1. **High resource utilization - significant impact on the database environment**
   2. **No separation of duties - ability of "super users" to bypass native auditing**
   3. **Inconsistent auditing features - difficulty of integrating auditing features of multiple database systems**

2. What is a rule and what is a policy?
   A rule is a set of filtering criteria and actions. A policy is a set of rules to be enforced.

© Copyright IBM Corporation 2011, 2013

Figure 1-20. Checkpoint solutions (1 of 2) GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (2 of 2)

3. Match the following Guardium components with their correct usage:

a) Real time monitoring	**d** Tracks changes to database setup files and security objects
b) Reporting	**f** Locates operating databases
c) Compliance Workflow Automation	**a** Performs database access filtering, alerting, and prevention
d) Configuration Auditing System	**g** Locates sensitive data
e) Vulnerability Assessment	**b** Generates built-in or custom documents
f) Database Discovery	**e** Tests to evaluate the overall security of the database environment
g) Data Classification	**c** Routes reports to users for comments and sign-off

© Copyright IBM Corporation 2011, 2013

Figure 1-21. Checkpoint solutions (2 of 2) GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 2. Guardium Architecture

Estimated time

00:30

What this unit is about

This unit describes how IBM InfoSphere Guardium goes about capturing database traffic.

What you should be able to do

After completing this unit, you should be able to:

- Identify the methods that Guardium uses to capture database traffic
- Describe aggregation and central management
- Understand the options to integrate Guardium with other tools
- Identify Guardium's hardware and software configuration

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Identify the methods that Guardium uses to capture database traffic
- Describe aggregation and central management
- Understand the options to integrate Guardium with other tools

© Copyright IBM Corporation 2011, 2013

Figure 2-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

2.1. Data collection methods

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data collection methods

After completing this topic, you should understand:

- Guardium's data collection methods:
  - SPAN ports
  - Network taps
  - STAP

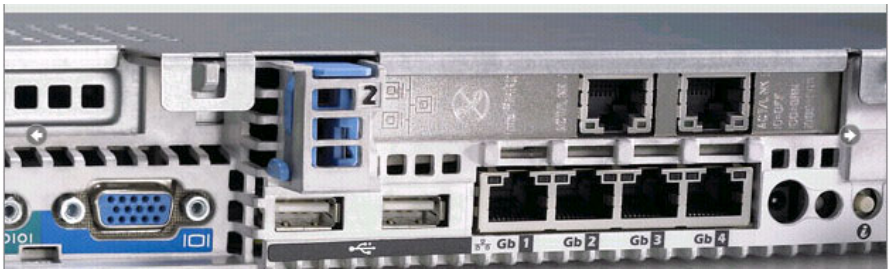
© Copyright IBM Corporation 2011, 2013

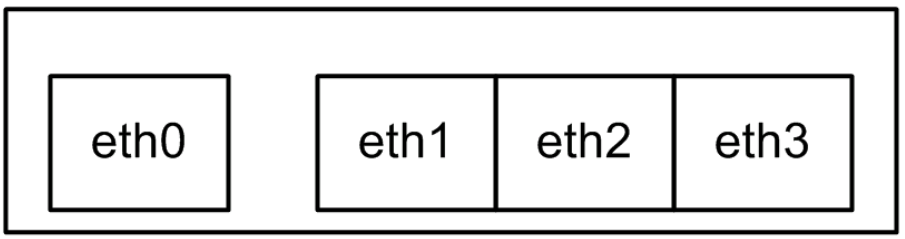
Figure 2-2. Data collection methods GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Collector





© Copyright IBM Corporation 2011, 2013

Figure 2-3. Collector GU2022.0

Notes:

The basic component of the InfoSphere Guardium solution is a network appliance called a ‘collector’.

The Collector

- is also called a G2000.
- is a hardened Linux server running on a Dell R610 computer with 12GB of RAM and a 300 GB hard drive.
- contains four network ports:
  - The management port, eth0, acts a standard network card. It has an IP address and is used the access the server over the network.
  - Eth1 through eth3 are configured as promiscuous by default. They do not have IP addresses and are designed to capture network traffic. However, one of these additional ports can be configured as a secondary network interface with an IP address, or can be used in network teaming.

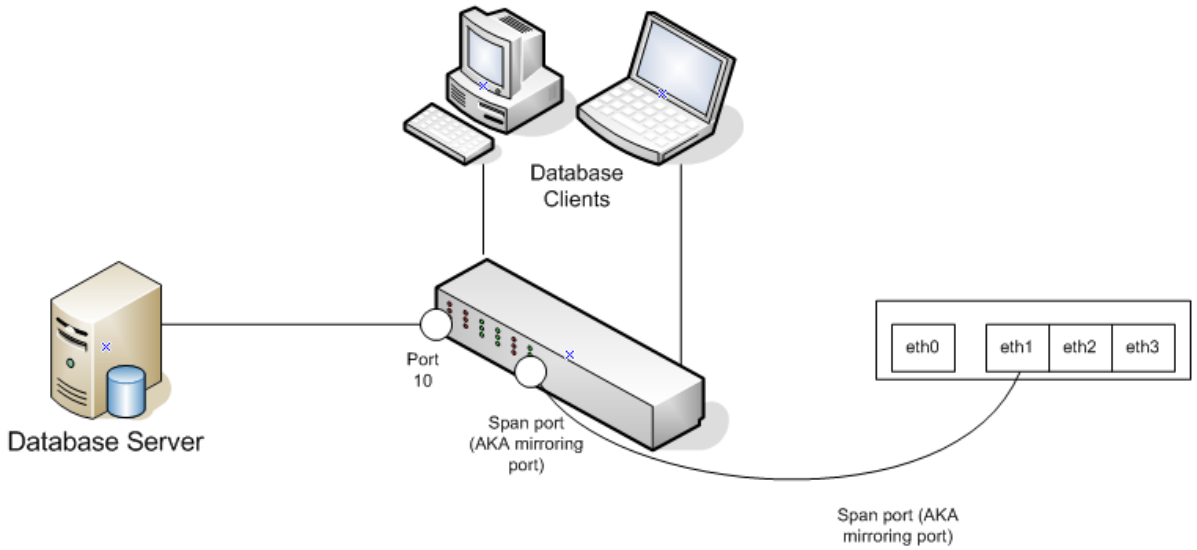
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Additional detail on the hardware options will be supplied later in this module.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Span port collection method



© Copyright IBM Corporation 2011, 2013

Figure 2-4. Span port collection method GU2022.0

Notes:

When the Guardium solution was first developed, the goal was to provide a completely passive (i.e. zero impact on the database server) method to monitor database activity by capturing the database activity from the network. The two most widely used methods for capturing network traffic are span ports and network taps.

Most modern network switches contain one or two ports (called span ports or mirroring ports) designated to monitor traffic on the switch. For the Guardium solution, these ports are configured to forward a copy of all traffic to and from a database server to one of the promiscuous ports on the Guardium appliance. Guardium receives an **exact copy** of all database traffic which it can digest and log it in its own internal database.

Advantages:

- No database downtime required
- Zero impact on the database server

Disadvantages:

- Local traffic is not captured

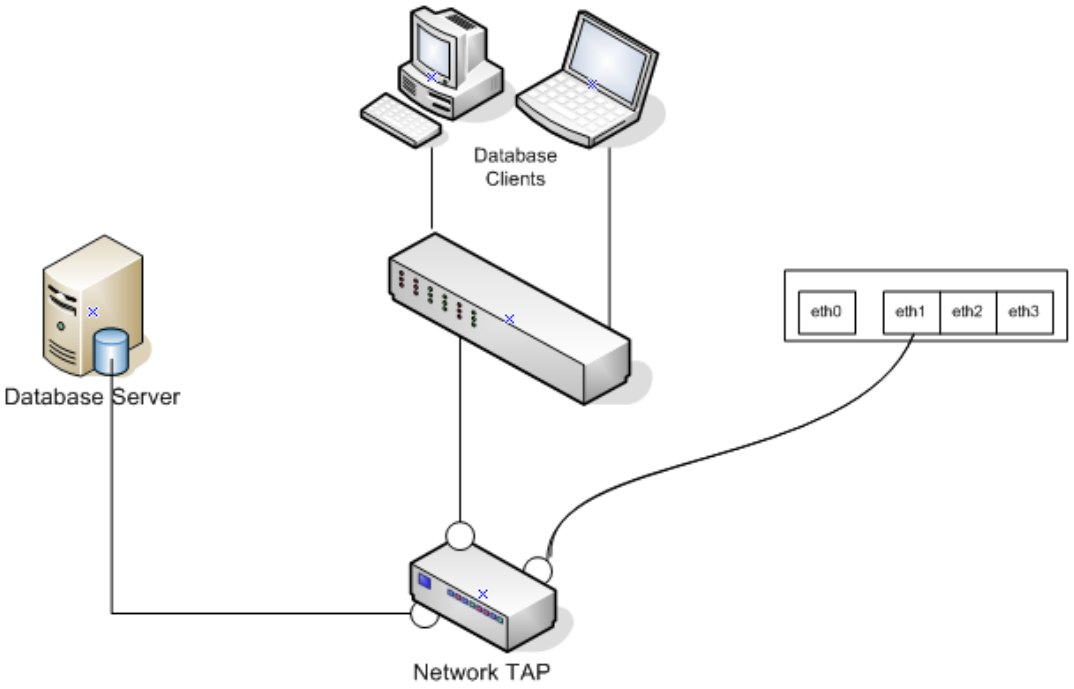
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Most switch vendors provide a limited number of SPAN ports
- Network administrators do not want to give up their available span ports
- If spanning several servers, extraneous traffic may be captured
- Contingency is difficult, if not impossible, to configure
- Encrypted traffic requires key management to be logged

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Network tap collection method



© Copyright IBM Corporation 2011, 2013

Figure 2-5. Network tap collection method GU2022.0

Notes:

Another common hardware solution is a network tap. The database server's network cable is connected to the network tap, not directly into the switch. The tap is then connected to the switch and to one (or possibly two) of the promiscuous ports on the Guardium collector. The network tap acts as a 'Y' connector – all traffic going to and from the database server also goes to the collector.

Advantages:

- No network reconfiguration needed
- Zero impact on the database server

Disadvantages:

- Server downtime is required
- Local activity is not captured
- Additional hardware cost
- Contingency is difficult, if not impossible, to configure

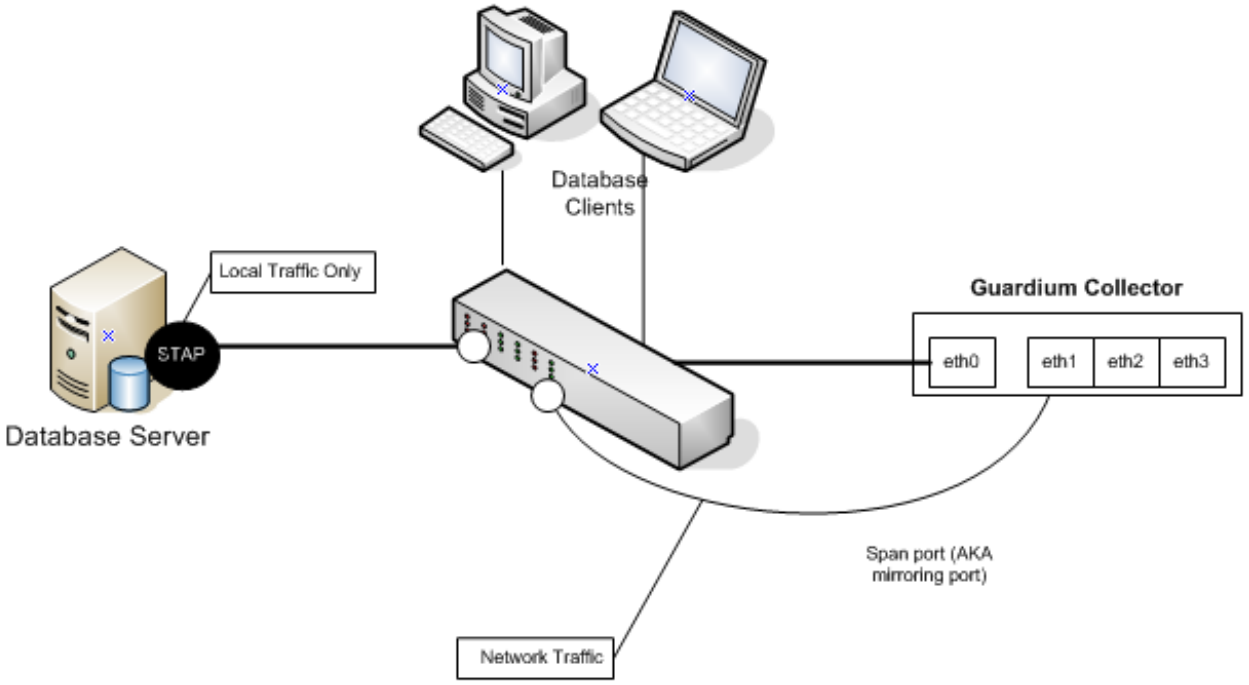
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Encrypted traffic requires key management to be logged

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

STAP: Local monitoring



© Copyright IBM Corporation 2011, 2013

Figure 2-6. STAP: Local monitoring GU2022.0

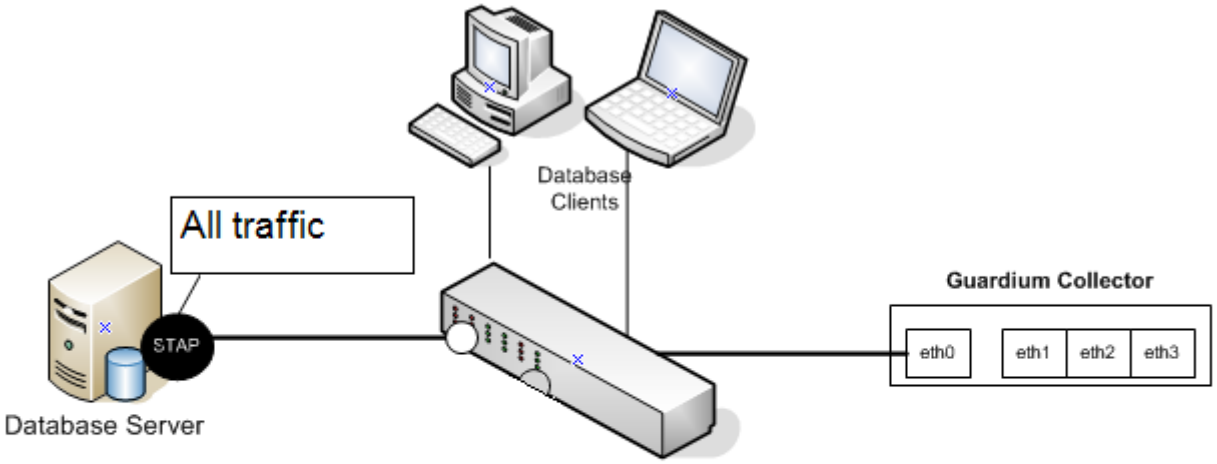
Notes:

Of all the disadvantages with span ports and network taps, the lack of local host monitoring is the most critical. To close this hole, Guardium developed a software agent, called an STAP (software tap), to forward local database activity to the collector. Local activity includes users directly accessing the system from a physically attached device, as well as those connecting via SSH (secure shell) or remote desktop.

Initially, STAP was meant to complement the hardware solutions. A span port or network tap would be used for network traffic, while STAP would be used for monitoring local traffic only. However, STAP always included the ability to forward network traffic as well, eliminating the need for a hardware solution.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

STAP: Local and network monitoring



© Copyright IBM Corporation 2011, 2013

Figure 2-7. STAP: Local and network monitoring GU2022.0

Notes:

Because the ease in using a software solution, as compared to hardware solutions, and the great increases in STAP's efficiency and sophistication, STAP has become the primary method of data capture for Guardium customers. Only a small percentage of customers still use span ports or network taps. However, it is still important to understand the hardware options, because STAP is basically a software implementation of the span port and/or network tap solution - STAP forwards network packets to the collector for logging.

STAP features:

- Light-weight agent running on the data server that forwards traffic, in the form of network packets, to a Guardium collector
- Minimal resource utilization
  - 3 to 5% CPU, 10 MB memory mapped file
- Encrypted Database traffic – handles most forms of database encryption (SSL, ASO, Kerberos, etc.)
- Redundancy – sends traffic to more than one collector

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Failover – provides failover to one or more collectors
- Load Balancing – sends traffic across multiple collectors
- Prevention – blocks activity or terminate connection
- Clusters – supports migrating, floating, unavailable databases
- Encryption – communicates over an encrypted channel to the collector (TLS)

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Raw network traffic

- The Guardium collector:
  - receives network and local traffic as raw data
  - parses and analyzes the data
  - logs the data in a MySQL database based on configured rules

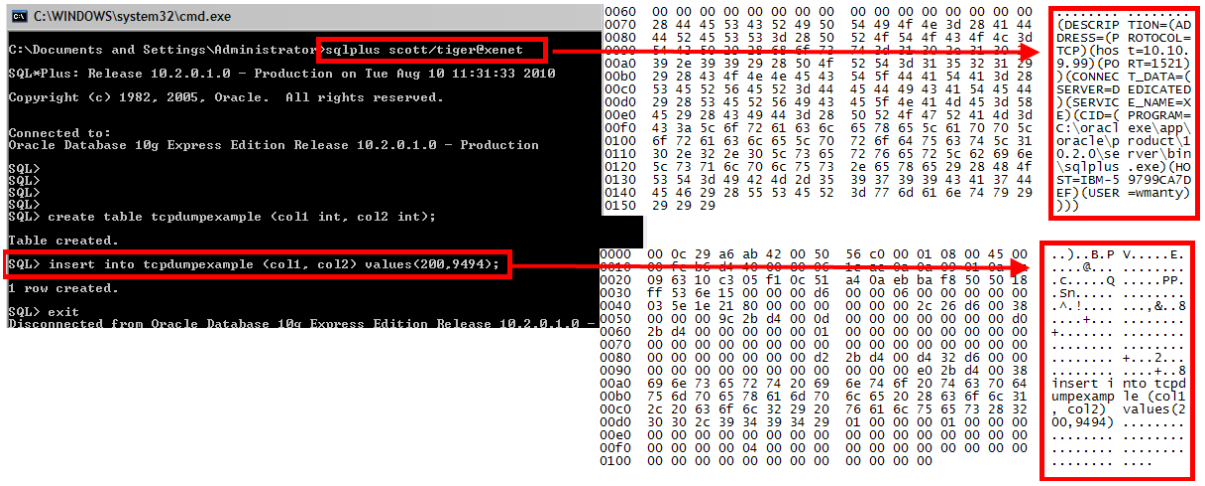

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>sqlplus scott/tiger@xenet
SQL*Plus: Release 10.2.0.1.0 - Production on Tue Aug 10 11:31:33 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL>
SQL>
SQL>
SQL>
SQL> create table tcpdumpexample (col1 int, col2 int);
Table created.
SQL> insert into tcpdumpexample (col1, col2) values(200,9494);
1 row created.
SQL> exit
Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 -

Figure 2-8. Raw network traffic GU2022.0

Notes:

The Guardium collector receives the traffic from the span ports and network taps as raw network traffic. A Linux process (the sniffer) on the collector parses this traffic, analyzes it, and logs it into an internal relational database on the Guardium appliance. The current database is a MySQL server.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should understand:

- Guardium's data collection methods, including:
  - SPAN ports
  - Network taps
  - STAP

© Copyright IBM Corporation 2011, 2013

Figure 2-9. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

2.2. Aggregation, Central Management, and Integration

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Aggregation, central management, and integration

After completing this topic, you should understand:

- Data aggregation
- Central management
- Hardware and software configuration options
- Integration options

© Copyright IBM Corporation 2011, 2013

Figure 2-10. Aggregation, central management, and integration GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Hardware and software

- **Collectors and Aggregators**
  - G2000 (Collector), G5000 (Aggregator)
  - Dell R610
  - 1U, Rack mountable
  - 12 GB RAM
  - 600 GB Hard drive with Raid 0 drive mirroring
- **Software**
  - Hardened Red Hat Enterprise Linux 5
  - MySQL database

© Copyright IBM Corporation 2011, 2013

Figure 2-11. Hardware and software GU2022.0

Notes:

Guardium appliances can be configured as collectors or as aggregators. The collectors are known as G2000s, and the aggregators are known as G5000s. The Guardium appliances are implemented on Dell R610 computers with 12 GB RAM and 600 GB Hard Disk. The appliances run a hardened version of Red Hat Enterprise Linux 5, and implement an internal MySQL relational database.

On the upcoming pages, various Guardium configurations will be discussed.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Collection

- A **collector** monitors and gathers data multiple database servers on multiple physical devices

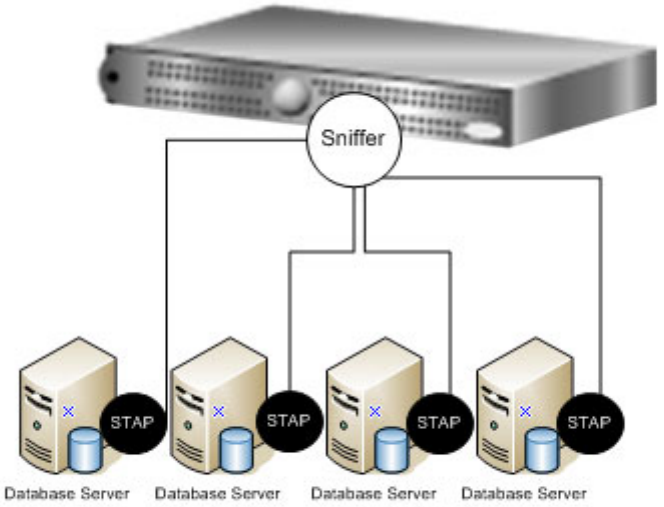


Figure 2-12. Collection GU2022.0

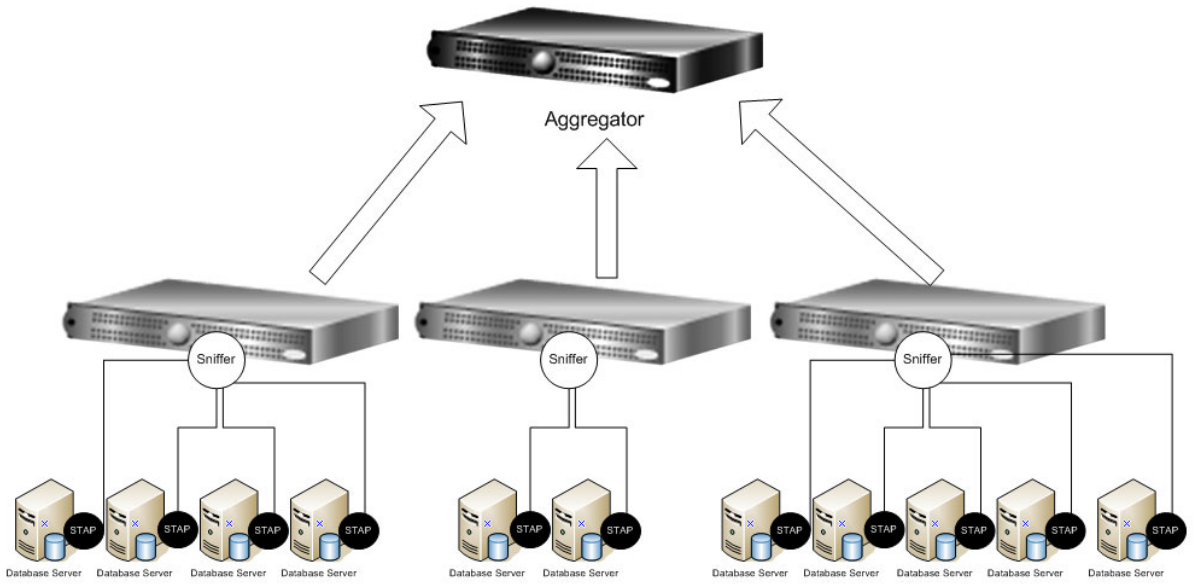
Notes:

A collector (also called a G2000) is one type of Guardium appliance. It collects traffic directly from database servers. One collector might monitor and gather data from one database server, or it might monitor and gather data from several database servers.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Aggregation

- An **aggregator** merges the data from multiple collectors into a single database.



© Copyright IBM Corporation 2011, 2013

Figure 2-13. Aggregation GU2022.0

Notes:

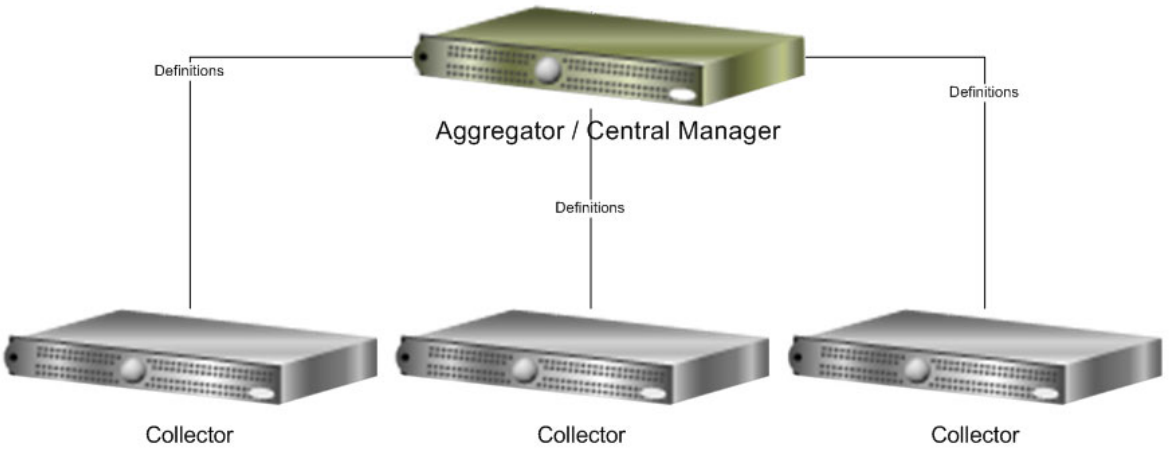
There are limits on the amount of traffic that a single collector can log effectively. After this limit has been reached, the internal buffers become full and the process that handles the traffic (that is, the sniffer) will restart, resulting in a loss of data. So, in many implementations, multiple collectors are required. The number of required collectors is usually a factor of the number of CPUs on each database server and the type and quantity of traffic to be monitored.

Whenever two or more collectors are utilized, one or more aggregators are included in the solution. An aggregator (also called a G5000) is a separate type of appliance. It does not collect traffic directly from database servers. Instead, each collector sends its data to an aggregator on a periodic basis (usually nightly). The aggregator then merges the data from all of the collectors into its own internal database. This allows users to view all of the data from multiple collectors in a central location.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Central management (1 of 2)

- One aggregator also functions as a **central manager**
- The central manager stores most definitions, including queries, reports, policies, and alerts



© Copyright IBM Corporation 2011, 2013

Figure 2-14. Central management (1 of 2) GU2022.0

Notes:

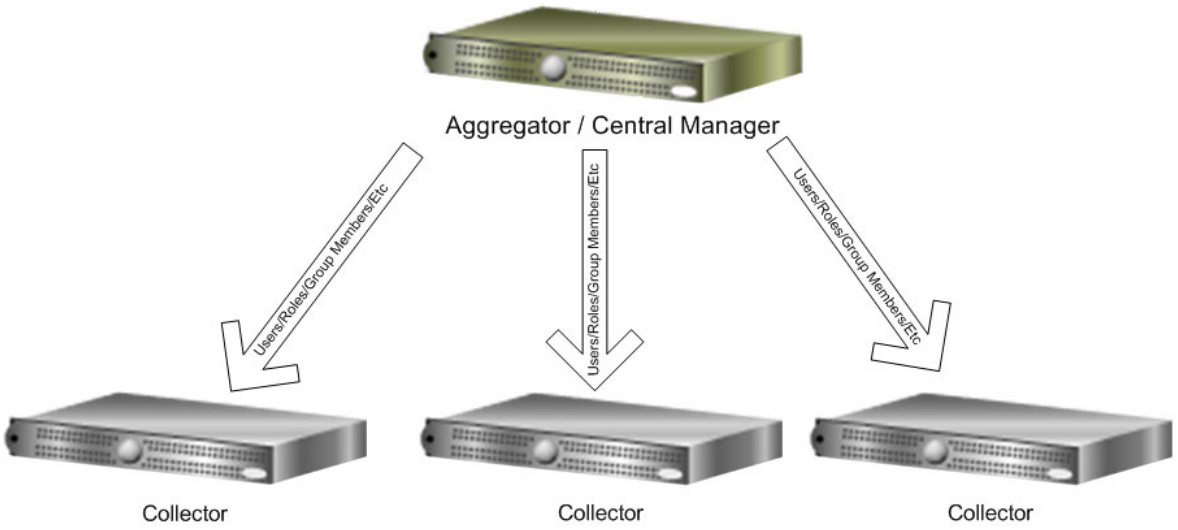
One aggregator also functions as a Central Manager. The Central Manager stores most definitions, including queries, reports, policies, and alerts. If a report is created on one collector, it is immediately available on all of the other appliances, including the Central Manager itself.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Central management (2 of 2)

- The central manager also defines users, roles, and other values, and “pushes” them down to the collectors



© Copyright IBM Corporation 2011, 2013

Figure 2-15. Central management (2 of 2) GU2022.0

Notes:

The Central Manager also provides a central location for the creation of users, roles, and other values. Users and roles can be managed on the Central Manager and pushed out to the managed units on a scheduled basis.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Small environments

- In a small environment, one appliance might act as both an aggregator and a central manager for the entire system

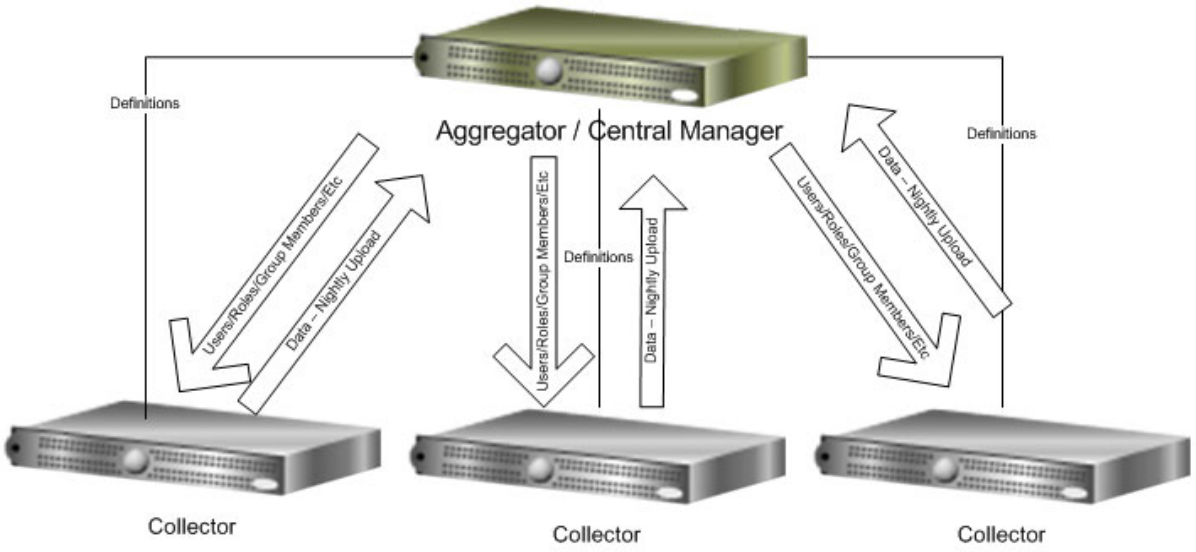


Figure 2-16. Small environments GU2022.0

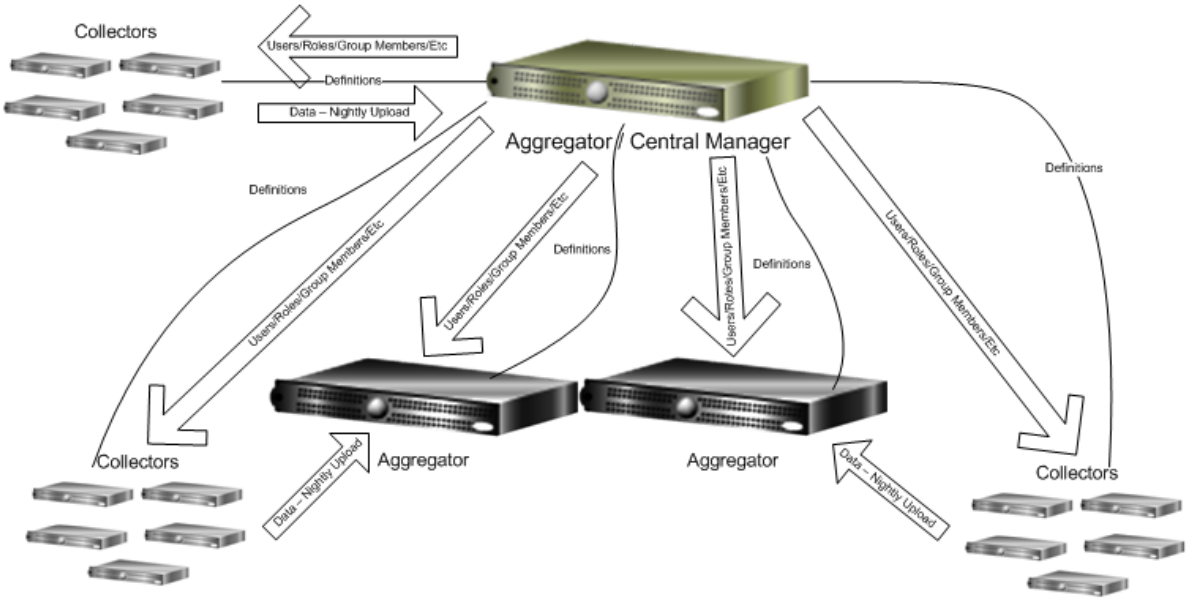
Notes:

A small environment might include just one Aggregator (which also acts as a Central Manager) that would handle all aggregation, definitions, and user management.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Medium-sized environments

- In a medium sized environment, the central manager might act as an aggregator in conjunction with other aggregators in the environment



© Copyright IBM Corporation 2011, 2013

Figure 2-17. Medium-sized environments GU2022.0

Notes:

In a medium-sized environment (usually 10 to 15 collectors), a Central Manager will continue to function as an aggregator for a subset of collectors and perform central management functions for all of the managed units (collectors and aggregators).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Larger-sized environments

- In a larger, enterprise environment, there may be a dedicated central manager that does not perform aggregation functions

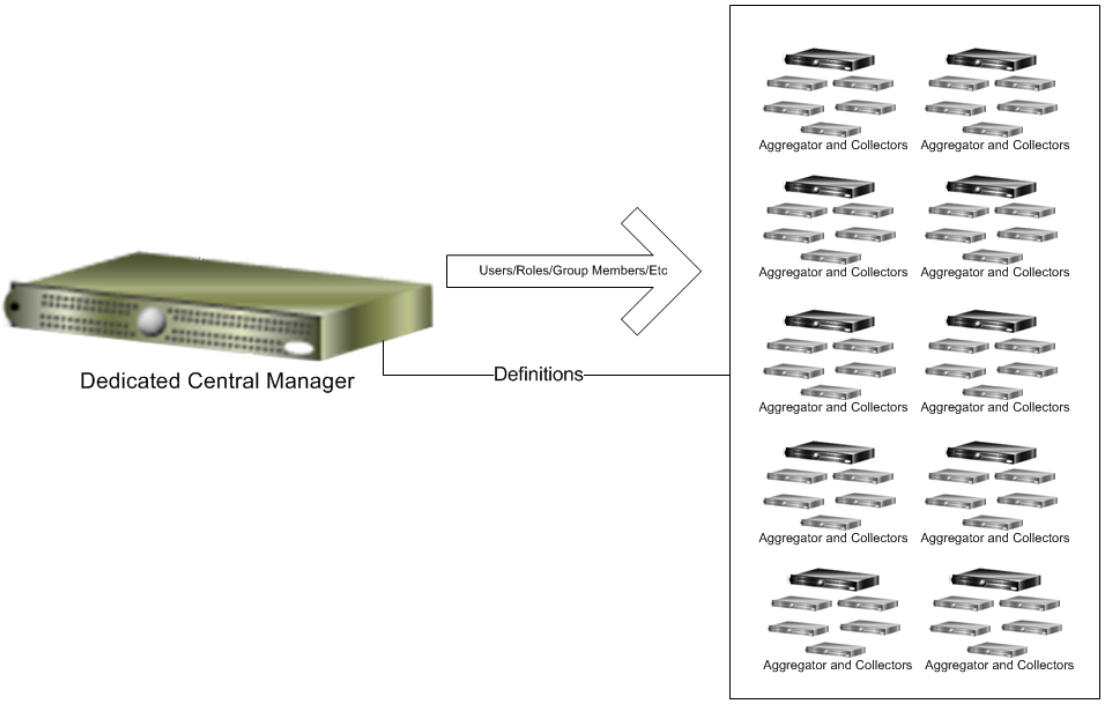


Figure 2-18. Larger-sized environments GU2022.0

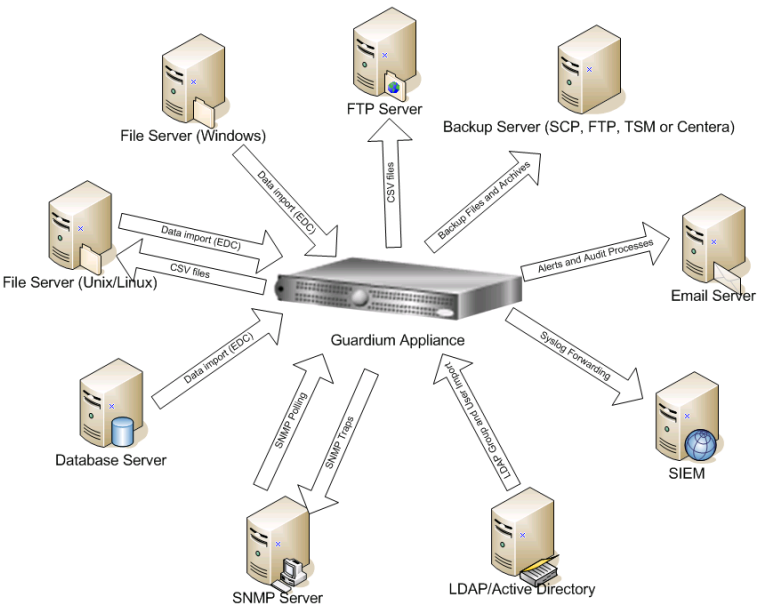
Notes:

In a enterprise-sized deployment (usually more than 10 to 15 collectors), the Central Manager will not function as an aggregator. Instead, it will be dedicated to central management functions only.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Integration

- The Guardium appliances interact with other servers in the network environment:
  - database servers
  - file servers
  - ftp servers
  - backup servers
  - email servers
  - other servers



© Copyright IBM Corporation 2011, 2013

Figure 2-19. Integration GU2022.0

Notes:

Guardium interacts with many other software servers in a corporate environment, including:

- Database servers
  - Data Access Monitoring (via STAP, SPAN port, or Network TAP)
  - Configuration Auditing System (CAS)
  - Enterprise Data Correlation (Guardium can upload data from external databases and integrate it into its internal database)
- File Servers
  - CSV exports (Unix Only)
  - Enterprise Data Correlation (Guardium can upload data from flat files and integrate it into its internal database)
- FTP Servers

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

  - CSV exports
- Backup Servers (SCP, FTP, TSM & Centera)
  - Daily Archives and System Backup
- Email Servers
  - Alerts and Audit Processes
- SIEM Servers
  - Alerts and reports send via Syslog forwarding
- LDAP/Active Directory Servers
  - Pass through authentication
  - Group member import
- SNMP servers
  - SNMP polling
  - SNMP traps

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Topic summary

Having completed this topic, you should understand:

- Data aggregation
- Central management
- Hardware and software configuration options
- Integration options

© Copyright IBM Corporation 2011, 2013

Figure 2-20. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. Guardium _____ are also known as G2000s and Guardium _____ are also known as G5000s.

2. True or False? The span port method and the network tap method monitor both local and network traffic.

3. Which operating system is used on the Guardium appliances?
   1. SUSE Linux
   2. Windows 8
   3. RedHat Enterprise Linux 5
   4. AIX

4. True or False? One collector can monitor and gather data from multiple database servers.

5. True or False? Guardium includes a built-in email server.

© Copyright IBM Corporation 2011, 2013

Figure 2-21. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

1. Guardium **collectors** are also known as G2000s and Guardium **aggregators** are also known as G5000s.
2. True or **False**? The span port method and the network tap method monitor both local and network traffic.
3. Which operating system is used on the Guardium appliances?
   a. SUSE Linux
   b. Windows 8
   c. **RedHat Enterprise Linux 5**
   d. AIX
4. **True** or False? One collector can monitor and gather data from multiple database servers.
5. True or **False**? Guardium includes a built-in email server.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Identify the methods that Guardium uses to capture database traffic
- Describe aggregation and central management
- Understand the options to integrate Guardium with other tools

© Copyright IBM Corporation 2011, 2013

Figure 2-22. Unit summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. Guardium **collectors** are also known as G2000s and Guardium **aggregators** are also known as G5000s.

2. True or **False**? The span port method and the network tap method monitor both local and network traffic.

3. Which operating system is used on the Guardium appliances?
   1. SUSE Linux
   2. Windows 8
   3. **RedHat Enterprise Linux 5**
   4. AIX

4. **True** or False? One collector can monitor and gather data from multiple database servers.

5. True or **False**? Guardium includes a built-in email server.

© Copyright IBM Corporation 2011, 2013

Figure 2-23. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Unit 3. Command Line Interface

Estimated time

00:30

What this unit is about

This unit give an introduction to the command line interface for IBM InfoSphere Guardium.

What you should be able to do

After completing this unit, you should be able to:

- Understand how to find the correct CLI commands appropriate to you needs
- Navigate the CLI
- Update the network configuration on an appliance
- Understand the GuardAPI

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand how to find the correct CLI commands appropriate to you needs
- Navigate the CLI
- Update the network configuration on an appliance
- Understand the GuardAPI

© Copyright IBM Corporation 2011, 2013

Figure 3-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI overview (1 of 2)

© Copyright IBM Corporation 2011, 2013

Figure 3-2. CLI overview (1 of 2) GU2022.0

Notes:

The Guardium appliance runs a hardened version of Red Hat Enterprise Linux. This means that no one, except perhaps a system administrator, has direct access to the operating system. Instead, all access to the appliance is through a tool called the Guardium Command Line Interface, or CLI. The CLI is an administrative tool that allows for configuration, troubleshooting, and management of the Guardium system. It is implemented using a Perl script, and includes a series of many commands that an administrator can use to view and configure settings in the Guardium appliance. The Perl script accepts **only** those command; no operating system commands are allowed.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI overview (2 of 2)

The CLI commands are arranged in 10 different categories:

- Network Configuration Commands
- Aggregator Commands
- Alerter Configuration Commands
- Configuration and Control Commands
- File Handling Commands
- Diagnostic Commands
- Inspection Engine Commands
- User Account, Password, and Authentication Commands
- Generate New Layout Command
- Certificate Commands

© Copyright IBM Corporation 2011, 2013

Figure 3-3. CLI overview (2 of 2) GU2022.0

Notes:

The CLI commands are grouped into 10 different categories.

CLI Command Catagories

1. Network Configuration
2. Aggregator
3. Alerter Configuration
4. Configuration and Control
5. File Handling
6. Diag(nostics)
7. Inspection Engine
8. User Account, Password, and Authenticatoin
9. New Layout
10. Certificate

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Each of these categories will be summarized later in this unit.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI users

- Default user accounts:
  - cli
  - guardcli1 through guardcli5
- cli logs on directly
- guardclix requires a second Guardium user id, entered via the “set guiuser” command
- set guiuser example:

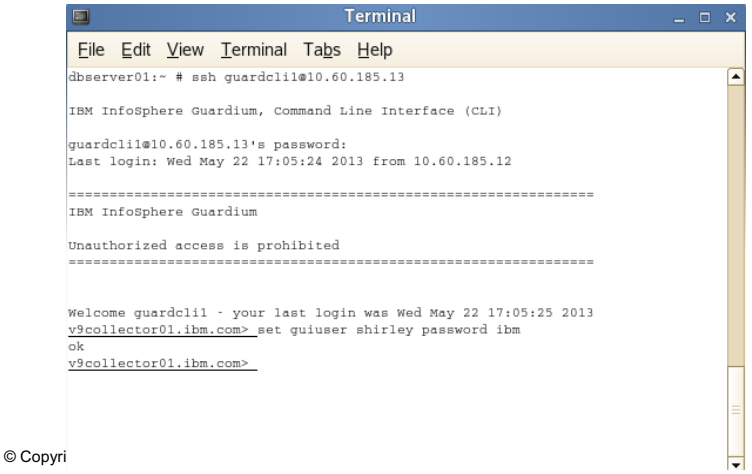

Terminal
File Edit View Terminal Tabs Help
dbserver01:~ # ssh guardcli1@10.60.185.13
IBM InfoSphere Guardium, Command Line Interface (CLI)
guardcli1@10.60.185.13's password:
Last login: Wed May 22 17:05:24 2013 from 10.60.185.12
IBM InfoSphere Guardium
Unauthorized access is prohibited
Welcome guardcli1 - your last login was Wed May 22 17:05:25 2013
v9collector01.ibm.com> set guiuser shirley password ibm
ok
v9collector01.ibm.com>
© Copyri

Figure 3-4. CLI users GU2022.0

Notes:

Access to the CLI and its commands is limited to a small group of Guardium users. The main administrator for the Guardium appliance would utilize the user id “cli”. Additionally, Guardium includes five other user accounts (guardcli1,..,guardcli5) which can be assigned to different users. These additional accounts provide for separate administration and better accountability.

Logging on to the CLI as the main administrative user cli requires only the appropriate password. Logging on to the CLI as one of the additional CLI accounts requires the appropriate password *AND* an additional user id and password. The additional user id and password are entered using the “set guiuser” command.

For example, to use one of the additional CLI user ids:

- Login via ssh as guardcli1.
- Issue the “set guiuser” command, passing in a second Guardium user id and password.

 © Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- The second Guardium user id must have either “admin” or “cli” as one of its roles to be able to utilize the CLI.

All activity performed by this login will be tracked as CLI_USER+GUI_USER (for example, guardcli+shirley) within Guardium’s internal audit trail.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI password requirements

All CLI accounts have the following password requirements:

- **Password Expiration:**
  - Enforced expiration periods (default = 90 days)
  - Required password change at next login
- **Password Validation:**
  - Minimum of eight characters in length
  - Contain at least one character from three of the following four classes:
    - Any upper case letter
    - Any lower case letter
    - Any numeric (0,1,2,...)
    - Any non-alphanumeric (special) character
- **LDAP**
  - CLI users **cannot** be authenticated through LDAP

© Copyright IBM Corporation 2011, 2013

Figure 3-5. CLI password requirements GU2022.0

Notes:

Guardium enforces password hardening on each of the CLI accounts (cli, and guardcli1 thru guardcli5). When installing (or rebuilding) a Guardium system from an installation DVD, the Guardium system will have a Guardium cli user with a default password of **guardium**. This password should be changed **immediately** to insure the security of the system.

All CLI accounts must abide by the following regulations:

- An expiration period for CLI passwords is enforced by the system. The default expiration period is 90 days. When a password expires, a required change of password will be invoked during the next login process.
- Passwords must be a minimum of eight characters in length, and must contain at least one character from three of the following four classes:
- Any upper case letter
- Any lower case letter
- Any numeric digit (0,1,2,...)

 © Copyright IBM Corp. 2011, 2013

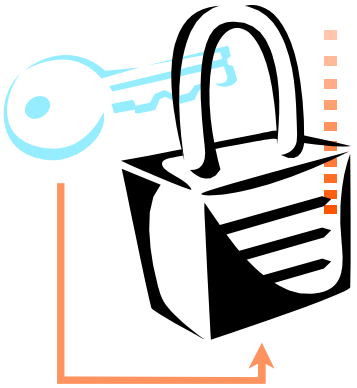
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Any non-alphanumeric (special) character (#, !, %, …)
- CLI users cannot be authenticated through LDAP as these are considered administrative accounts and should be able to login regardless of connectivity to an LDAP server
- As mentioned earlier, the special CLI accounts guardcli1 through guardcli5 require use of an additional user id. The CLI audit trail will show the CLI account (CLI_USER) and the additional account (GUI_USER) in all entries generated for the user.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI user login (1 of 2)

- The CLI user login is always a secure login
- It can be done one of three ways:
  - Through the console on the Guardium appliance
  - Through an ssh (security shell) connection
  - Through an ssh tool (such as Putty or SecureCRT)



© Copyright IBM Corporation 2011, 2013

Figure 3-6. CLI user login (1 of 2) GU2022.0

Notes:

Logging on with one of the CLI accounts is **always** done through a secure connection. If the user has physical access to the Guardium appliance, the logon can be through the system console or through a terminal connected through the serial port. The user can also logon through a secure connection using an ssh (secure shell) client. Common ssh tools include Putty and SecureCRT.

 © Copyright IBM Corp. 2011, 2013

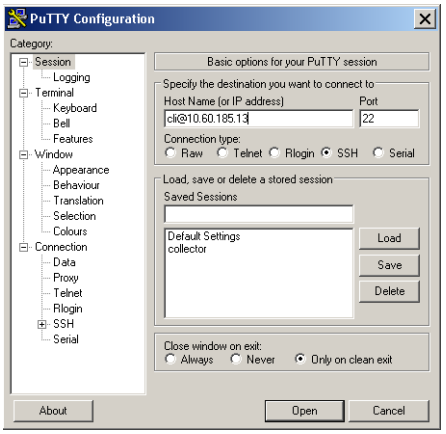
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CLI user login (2 of 2)

Console

```
==========================================================
SQL Guard 8.0 ----------------------

Unauthorized access is prohibited
==========================================================
guard login: cli
Password:
Last login: Fri Oct  1 11:00:24 on tty1
Welcome cli - this is your first login in this system.
Your password has expired.
Changing password for 'cli'.
Enter current password:
Enter new password:
Re-enter new password:
Setting default expiration period to 90 days.
```

Putty



Terminal

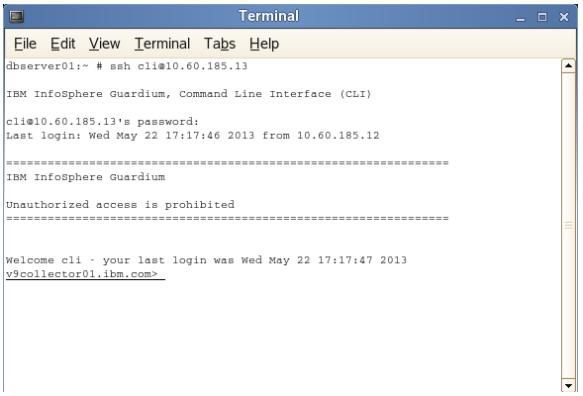

Terminal
File Edit View Terminal Tabs Help
dbserver01:~ # ssh cli@10.60.185.13
IBM InfoSphere Guardium, Command Line Interface (CLI)
cli@10.60.185.13's password:
Last login: Wed May 22 17:17:46 2013 from 10.60.185.12
IBM InfoSphere Guardium
Unauthorized access is prohibited
Welcome cli - your last login was Wed May 22 17:17:47 2013
v9collector01.ibm.com>

Figure 3-7. CLI user login (2 of 2) GU2022.0

Notes:

Three secure logons are demonstrated on this slide. The secure logon can be done physically from the Guardium appliance's console; through a secure Putty connection; or through a secure ssh connection from a Unix terminal window.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Navigating the CLI (1 of 4)

- Commands and keywords can be abbreviated by entering enough characters so the commands are unambiguous.
- Most Guardium CLI commands consist of a command word followed by one or more arguments. The argument may be a keyword or a keyword followed by a variable value.
- Commands and keywords are not case sensitive, but element names are.
- Quotation marks are used around words or phrases to precisely define search terms.

© Copyright IBM Corporation 2011, 2013

Figure 3-8. Navigating the CLI (1 of 4) GU2022.0

Notes:

CLI commands follow some standard usage conventions:

- Commands and keywords can be abbreviated by entering enough characters so the commands are unambiguous.
- Most Guardium CLI commands consist of a command word followed by one or more arguments. The argument may be a keyword or a keyword followed by a variable value.
- Commands and keywords are not case sensitive, but element names are.
- Quotation marks are used around words or phrases to precisely define search terms.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Additional information — If time permits, have the students login as the cli user and run some of the commands on this and the following slides. Make sure that they do not run 'restart system' as this will reboot their virtual machines.

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Navigating the CLI (2 of 4)

- To generate a list of all available commands for a given topic, type **command (**or **comm)** plus a keyword or part of a keyword
  - For example, **comm file** will return all file handling commands

```
v9collector01.ibm.com> comm file
aggregator backup keys file
aggregator restore keys file
export file
fileserver
import file
show backup profile
show system cpu profile
show timeout fileserver_session
store backup profile
store system cpu profile
store timeout fileserver_session
support clean log_files
support show large_files
ok
```

© Copyright IBM Corporation 2011, 2013

Figure 3-9. Navigating the CLI (2 of 4) GU2022.0

Notes:

To generate a list of all available commands for a given category, type **command** (or **comm**) plus a keyword or part of a keyword at the command prompt. For example, **comm agg** will return all aggregation related commands; **comm net** will return all network related commands; **comm file** will return all file handling commands; and so on.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Additional information — If time permits, have the students login as the cli user and run some of the commands on this and the following slides. Make sure that they do not run 'restart system' as this will reboot their virtual machines.

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Navigating the CLI (3 of 4)

- To display command syntax and usage options, enter a question mark (?) as an argument following the command word.
  - For example, **supp show ?** will display all of the options for the support show command

```
v9collector01.ibm.com> supp show ?
USAGE:  support show <arg>, where arg is:
audit_tasks, db-processlist, db-status, db-struct-check, db-top-ta
bles, hardware-info, iptables, large_files, netstat, passkey, slow
_log, top
v9collector01.ibm.com>
```

© Copyright IBM Corporation 2011, 2013

Figure 3-10. Navigating the CLI (3 of 4) GU2022.0

Notes:

To display command syntax and usage options, enter a question mark (?) as an argument following the command word or words. For example:

agg list ?

supp show ?

show ?

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Navigating the CLI (4 of 4)

- Another way of getting all possible arguments for a command is to enter the first word (or words) of the command.

  Examples:

  - **show system**

```
v9collector01.ibm.com> show system
USAGE:  show system <arg>, where arg is:
?, apc, banner, certificate, clock, conntrack, cpu, custom_db_max_size, custom_db
_usage, domain, fullname, hostname, issue, key, netfilter-buffer-size, ntp, patch
, public, remote-root-login, scheduler, snif-buffers-reclaim, snmp
```

  - **stop**

```
v9collector01.ibm.com> stop
USAGE:  stop <arg>, where arg is:
?, alerter, gui, inspection-core, inspection-engines, system
```

© Copyright IBM Corporation 2011, 2013

Figure 3-11. Navigating the CLI (4 of 4) GU2022.0

Notes:

An alternate method of getting all possible arguments for a command is to enter the first word (or words) of the command at the command prompt. For example:

agg list

supp show

show

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Show and store

- The SHOW command displays the value of the indicated argument
- The STORE command changes the value of the indicated argument
  - Examples
    - SHOW PASSWORD EXPIRATION GUI

```
v9collector01.ibm.com> show password expiration gui
Password expires after 90 days.
ok
```

    - STORE PASSWORD EXPIRATION GUI 100

```
v9collector01.ibm.com> store password expiration gui 100
ok
```

    - SHOW PASSWORD EXPIRATION GUI

```
v9collector01.ibm.com> show password expiration gui
Password expires after 100 days.
ok
```

© Copyright IBM Corporation 2011, 2013

Figure 3-12. Show and store GU2022.0

Notes:

The SHOW command displays the value of the indicated argument, and the STORE command changes the value of the indicated argument.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Reminder: CLI command categories

The CLI commands are arranged in 10 different categories:

- Network Configuration Commands
- Aggregator Commands
- Alerter Configuration Commands
- Configuration and Control Commands
- File Handling Commands
- Diagnostic Commands
- Inspection Engine Commands
- User Account, Password, and Authentication Commands
- Generate New Layout Command
- Certificate Commands

© Copyright IBM Corporation 2011, 2013

Figure 3-13. Reminder: CLI command categories GU2022.0

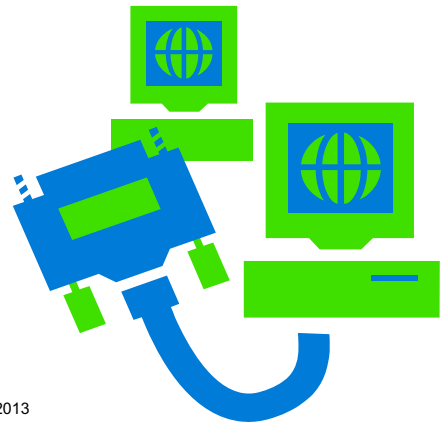
Notes:

The CLI commands are grouped into 10 different categories. We will now take a very high level look at each of these categories.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Network configuration commands

- Use the network configuration CLI commands to:
  - Identify a connector on the back of the appliance
  - Reset networking after installing or moving a network card
  - Set IP addresses
  - Enable or disable high-availability
  - Configure the network card if the switch it attaches to will not auto-negotiate the settings
  - And so on



© Copyright IBM Corporation 2011, 2013

Figure 3-14. Network configuration commands GU2022.0

Notes:

When an InfoSphere Guardium appliance is first received, it must be racked, powered, and connected to the network. Once the appliance is physically connected, it must be initially configured to make it accessible over the network. This configuration will need to be completed with physical access to the appliance or remotely through a KVM solution or an optional DRAC card installed in the appliance.

- The following commands are used to configure to configure the network:
  - store network interface ip <ip_address>
  - store network interface mask <subnet_mask>
  - store network routes def <default_router_ip>
  - store network resolver 1 <resolver_1_ip>
  - store network resolver 2 <resolver_2_ip>
  - store network resolver 3 <resolver_3_ip>
  - store system hostname <host_name>

 © Copyright IBM Corp. 2011, 2013

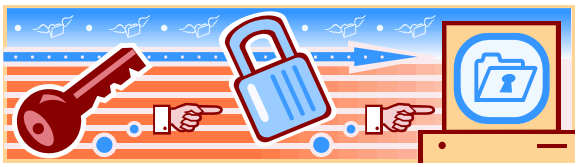
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

  - store system domain <domain_name>
- After the configuration has been completed, a “restart system” must be performed.
- After the system has rebooted, connectivity can be confirmed with the following commands:
  - ping <default_router_ip>
  - ping <resolver_1_ip>

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Aggregator commands

- Use the aggregator CLI commands to:
  - Back up the shared secret keys file to a specified location
  - Define the amount of collector data that the aggregator UI will work with
  - Set the system shared secret key to null
  - Start or stop writing debug information related to aggregator activities
  - Move or rename failed import files
  - And so on



© Copyright IBM Corporation 2011, 2013

Figure 3-15. Aggregator commands GU2022.0

Notes:

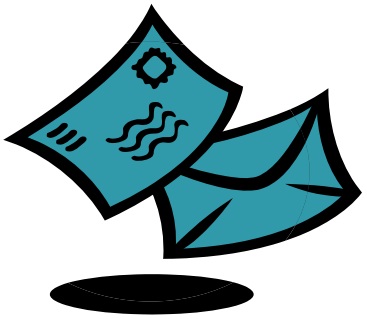
Aggregation is the process by which export files are sent from each collector to an aggregator, where the data from all of the collectors is merged and stored in a single database. This provides a single reporting source for all of the monitored data.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Alerter configuration commands

- Use the alerter configuration CLI commands to:
  - Stop or restart the alerter
  - Specify that the alerter will be started automatically whenever the system is rebooted
  - Set the polling interval for the alerter
  - Set the alerter's SMTP authentication password
  - Set the alerter's SMTP email authentication username
  - And so on



© Copyright IBM Corporation 2011, 2013

Figure 3-16. Alerter configuration commands GU2022.0

Notes:

The Alerter subsystem transmits messages that have been queued by other components; for example, correlation alerts that have been queued by the Anomaly Detection subsystem, or run-time alerts that have been generated by security policies. The Alerter subsystem can be configured to send messages to both SMTP and SNMP servers. Alerts can also be sent to syslog or custom alerting classes, but no special configuration is required for those two options beyond starting the Alerter.

The Alerter can be configured in the GUI under Administration Console > Configuration > Alerter

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration and control commands

- Use the configuration and control CLI commands to:
  - Check the installed licenses
  - Ping remote systems
  - Restart the GUI interface
  - Reboot the Guardium appliance
  - Set the user timeout value
  - And so on

© Copyright IBM Corporation 2011, 2013

Figure 3-17. Configuration and control commands GU2022.0

Notes:

The configuration and control CLI commands cover a large number of configuration settings within the Guardium appliance. Remember that the STORE command is used to set a configuration setting, and the SHOW command is used to display a current configuration setting.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

File handling commands

- Use the file handling CLI commands to:
  - Backup and restore configuration information
  - Backup and restore the Guardium database
  - Backup and restore profile information
  - Export and import audit data
  - Display exported audit data files
  - And so on

© Copyright IBM Corporation 2011, 2013

Figure 3-18. File handling commands GU2022.0

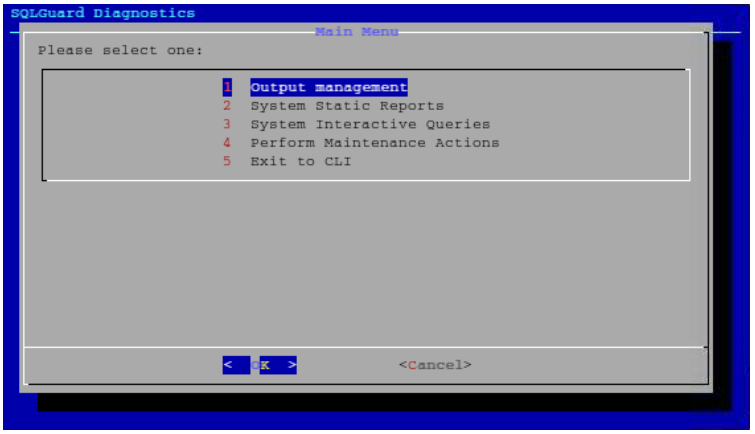
Notes:

The file handling commands are used to work with the Guardium files, including the configuration files, the database files, the profiles, auditing files, and so on.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Diagnostic commands

- The **diag** command will bring up a menu-driven window that will allow you perform a number of diagnostic functions.
- There are no functions that you would perform with the **diag** command on a regular basis.
- Generally, you would use this command only as directed by Technical Support.



© Copyright IBM Corporation 2011, 2013

Figure 3-19. Diagnostic commands GU2022.0

Notes:

The diagnostic commands are used only under the direction of Technical Support.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Inspection engine commands

- Use the inspection engine CLI commands to:
  - Add an inspection engine
  - Delete an inspection engine
  - List inspection engines
  - Stop and restart an inspection engine
  - And so on

© Copyright IBM Corporation 2011, 2013

Figure 3-20. Inspection engine commands GU2022.0

Notes:

An **inspection engine** monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example). The inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User account, password, and authentication commands

- Use the user account, password, and authentication CLI commands to:
  - Define when an inactive user account will be disabled
  - Define when a password must be changed
  - Lockout users after failed login attempts
  - Enable and disable password validation
  - And so on

© Copyright IBM Corporation 2011, 2013

Figure 3-21. User account, password, and authentication commands GU2022.0

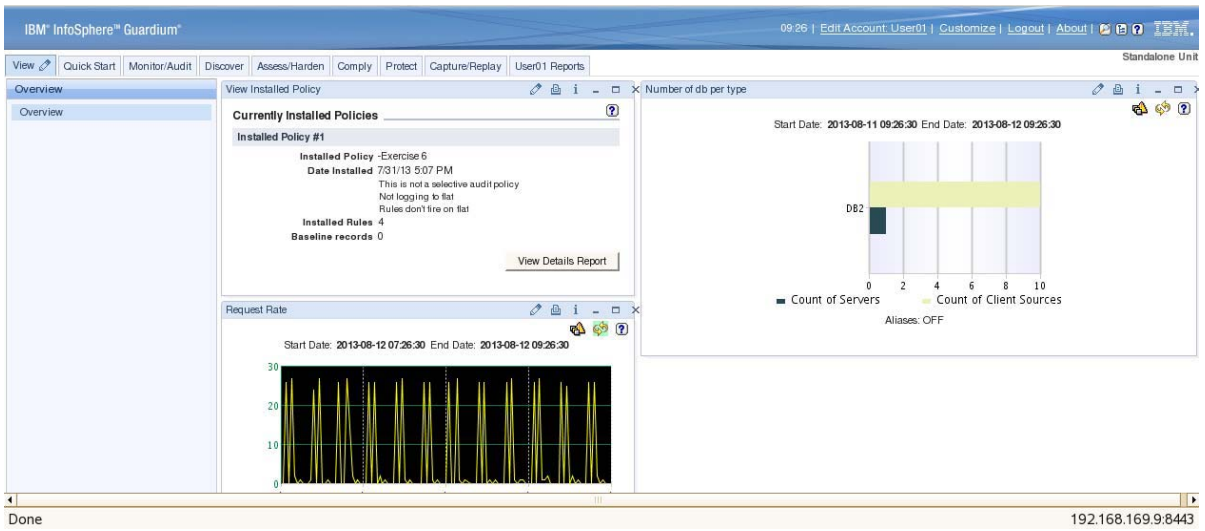
Notes:

The user account, password, and authentication commands work with user account information.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Generate new layout command

- The generate new layout command generates a new web GUI layout for an existing role.



© Copyright IBM Corporation 2011, 2013

Figure 3-22. Generate new layout command GU2022.0

Notes:

The Guardium portal window (web interface GUI) contains one or more panes (or tabs). Each pane defines the layout of some portion of the window. Each pane may contain one or more other panes. The Guardium administrator or access manager can generate, via the CLI, a default layout for a role. After that, any new user who is assigned that role will have that layout after logging in for the first time.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Certificate commands

- Use the certificate CLI commands to:
  - Create a certificate signing request (CSR)
  - Store a CA (Certificate Authority) or intermediate trusted path certificate on the Guardium appliance
  - Store a server certificate on the Guardium appliance
  - Create a Certificate Signing Request in PEM format

© Copyright IBM Corporation 2011, 2013

Figure 3-23. Certificate commands GU2022.0

Notes:

The certificate commands are used to create a certificate signing request (CSR); and to install server, CA, or trusted path certificates on the Guardium appliance.

Note: Guardium does not provide Certificate Authority (CA) services and will not ship systems with certificates that differ from the one installed by default. A customer that wants their own certificate will need to contact a third party CA (such as VeriSign or Entrust).

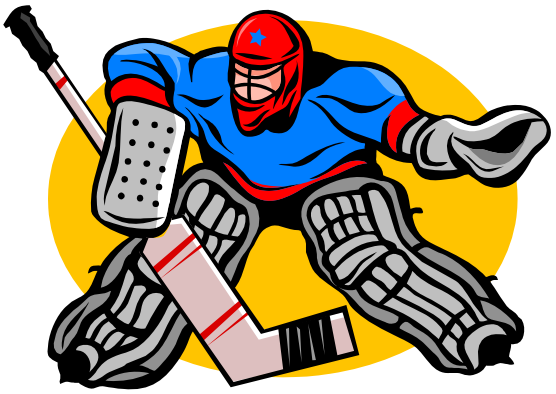
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GuardAPI (1 of 2)

- GuardAPI is a set of CLI commands that provide access to Guardium functionality from the command line.
  - Allows for the automation (or scripting) of repetitive tasks

- GuardAPI covers the following functions:
  - CAS
  - Catalog Entry
  - Datasource
  - Datasource Reference
  - Group
  - Role
  - S-TAP
  - Process control



© Copyright IBM Corporation 2011, 2013

Figure 3-24. GuardAPI (1 of 2) GU2022.0

Notes:

GuardAPI provides access to Guardium functionality from the command line or from scripted files. This allows for the automation of repetitive tasks, which is especially valuable in larger implementations. Calling these GuardAPI functions enables a user to quickly perform operations such as creating datasources, maintaining user hierarchies, or maintaining Guardium features such as S-TAP.

GuardAPI includes a set of CLI commands, all of which begin with the keyword **grdapi**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GuardAPI (2 of 2)

- Use **grdapi commands** to list all of the GuardAPI commands

```
v9collector01.ibm.com> grdapi commands
ID=0
API Function list :
add_approved_stap_client
add_assessment_datasource
add_assessment_test
add_autodetect_task
add_receiver_to_rule_action
add_time_period
change_rule_order
clear_cas_template_set
clone_cas_template_set
close_default_events
copy_rule
copy_rules
create_ad_hoc_audit_and_run_once
create_api_parameter_mapping
create_assessment
create_autodetect_process
create_cas_host_instance
create_cas_template
create_cas_template_set
......
```

© Copyright IBM Corporation 2011, 2013

Figure 3-25. GuardAPI (2 of 2) GU2022.0

Notes:

- To list all GuardAPI commands available, enter the **grdapi** command with no arguments or use the **'grdapi commands'** command with no search argument.
- To display the parameters for a particular command, enter the command followed by '--help=yes'.
- To search for GuardAPI commands given a search string use the '**grdapi commands *<search-string>***' command structure.
- To display a values list for a parameter, enter the command followed by '--get_param_values=<parameter>'.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1) How does the CLI user differ from the GUARDCLI1 user?

2) True or False? CLI users can be authenticated through LDAP.

3) List three ways a CLI user can make a logon connection with the Guardium appliance.

4) What CLI command could you use to list all of the commands that fall into the Aggregator category?

5) The ___ command is used to display the value of a Guardium configuration option. The ____ command is used to set the value of a Guardium configuration option.

6) Which Guardium CLI command is normally used only under the guidance of Technical Support?

7) The commands needed for repetitive tasks can be automated using _____.

© Copyright IBM Corporation 2011, 2013

Figure 3-26. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

6.

7.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers:

1. How does the CLI user differ from the GUARDCLI1 user?

   The CLI user signs on with a password; the guardcli1 user signs on with a password and then issues the set guiuser command to complete the logon.

2. True or **False**? CLI users can be authenticated through LDAP.
3. List three ways a CLI user can make a logon connection with the Guardium appliance.

   Console, ssh, ssh tool like Putty

4. What CLI command could you use to list all of the commands that fall into the Aggregator category?

   comm agg

5. The **show** command is used to display the value of a Guardium configuration option. The **store** command is used to set the value of a Guardium configuration option.
6. Which Guardium CLI command is normally used only under the guidance of Technical Support?

   Diag

7. The commands needed for repetitive tasks can be automated using

   GuardAPI.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand how to find the correct CLI commands appropriate to you needs
- Navigate the CLI
- Update the network configuration on an appliance
- Understand the GuardAPI

© Copyright IBM Corporation 2011, 2013

Figure 3-27. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 1** in the Exercise Guide.

© Copyright IBM Corporation 2012, 2013

Figure 3-28. Exercise GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1) How does the CLI user differ from the GUARDCLI1 user? **The CLI user signs on with a password; the guardcli1 user signs on with a password and then issues the set guiuser command to complete the logon**.

2) True or **False**? CLI users can be authenticated through LDAP.

3) List three ways a CLI user can make a logon connection with the Guardium appliance. C**onsole, ssh, ssh tool like Putty**

4) What CLI command could you use to list all of the commands that fall into the Aggregator category? **comm agg**

5) The **show** command is used to display the value of a Guardium configuration option. The **store** command is used to set the value of a Guardium configuration option.

6) Which Guardium CLI command is normally used only under the guidance of Technical Support? **diag**

7) The commands needed for repetitive tasks can be automated using **GuardAPI**.

© Copyright IBM Corporation 2011, 2013

Figure 3-29. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 4. Access Management

Estimated time

00:30

What this unit is about

This unit describes how to define new Guardium users and assign those user to roles.

What you should be able to do

After completing this unit, you should be able to:

- Create new users
- Assign roles to new users

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Create new users
- Assign roles to new users

© Copyright IBM Corporation 2011, 2013

Figure 4-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

accessmgr

- accessmgr:
  - Is a built-in user
  - Is automatically in the access management role
  - Cannot be deleted
  - Can create and maintain user accounts and roles
  - Provides for separation of duties

© Copyright IBM Corporation 2011, 2013

Figure 4-2. accessmgr GU2022.0

Notes:

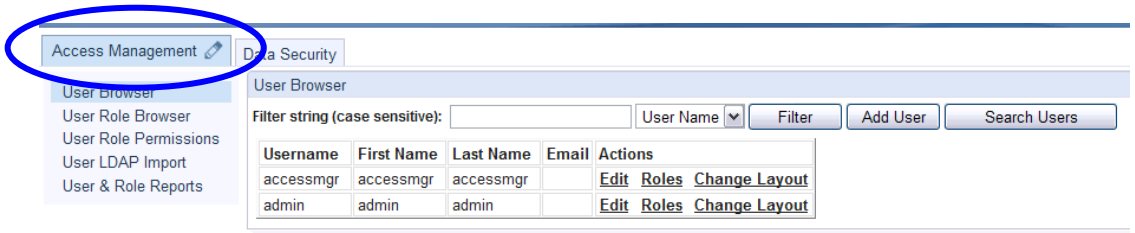
One of the two major built-in users in Guardium is the user named “accessmgr” (pronounced Access Manager). The Access Manager’s primary functions are to create and maintain user accounts and roles.

Access management functions (create users, change passwords, etc) are performed by users in the access management role. Access Manager (the user) is automatically part of the access management role. Admin (the user) is **not** automatically part of the access management role. This allows for the separation of system duties between the administrator (admin) and the access manager (accessmgr).

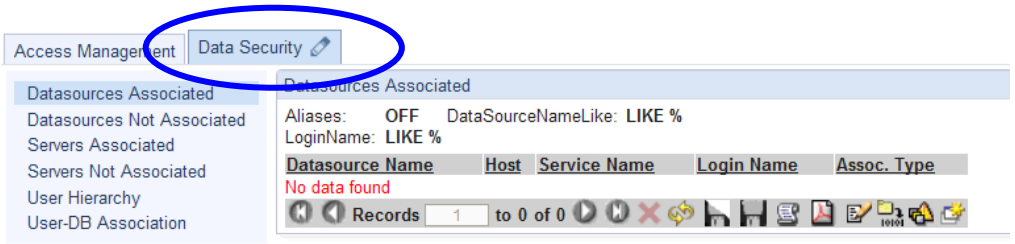
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Management GUI panes

- The access management GUI screen layout includes two panes:
  - **Access Management**



  - **Data Security**



© Copyright IBM Corporation 2011, 2013

Figure 4-3. Access Management GUI panes GU2022.0

Notes:

The GUI layout for users in the access management role include two panes: Access Management and Data Security. The functions on these two panes will be discussed on the next few pages.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Management tab

The **Access Management** pane contains all of the links required to manage users, roles, and access to applications, including:

- User Browser
- User Role Browser
- User Role Permissions
- User LDAP Import
- User & Role Reports

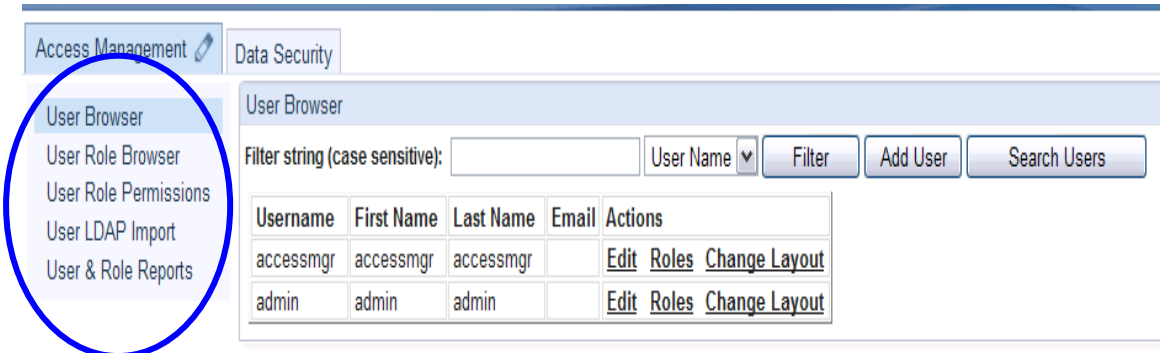


Figure 4-4. Access Management tab GU2022.0

Notes:

The **Access Management** pane menu contains all of the links required to manage users, roles, and access to applications, and will be covered in detail in this unit. Access Management contains the following menu items:

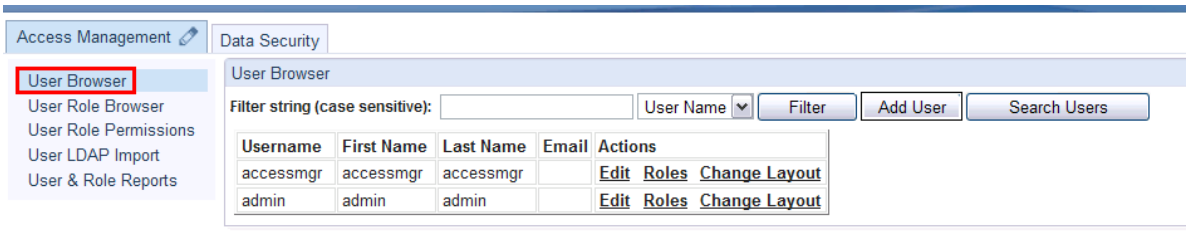
- User Browser
- User Role Browser
- User Role Permissions
- User LDAP Import
- User & Role Reports

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser

- The **User Browser** link is used to create, modify, and delete Guardium user accounts.



© Copyright IBM Corporation 2011, 2013

Figure 4-5. User Browser GU2022.0

Notes:

The User Browser link is used to create, modify, and delete Guardium user accounts. Anyone in the access management role has access to this pane, and can work with user ids. There are options to find users, add users, edit users, delete users (except for accessmgr and admin), and to change a user's GUI layout.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

If time allows, have the students follow along from their virtual machines.

Purpose —

Details —

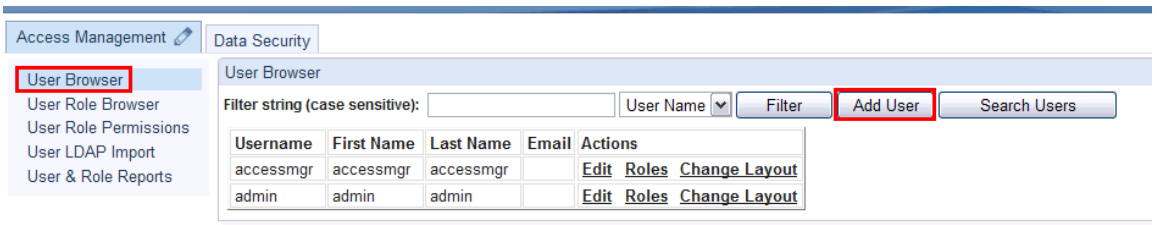
Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser - adding a user (1 of 2)

- The **Add User** button is used to create, modify, and delete Guardium user accounts.



© Copyright IBM Corporation 2011, 2013

Figure 4-6. User Browser - adding a user (1 of 2) GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

If time allows, have the students follow along from their virtual machines.

Purpose —

Details —

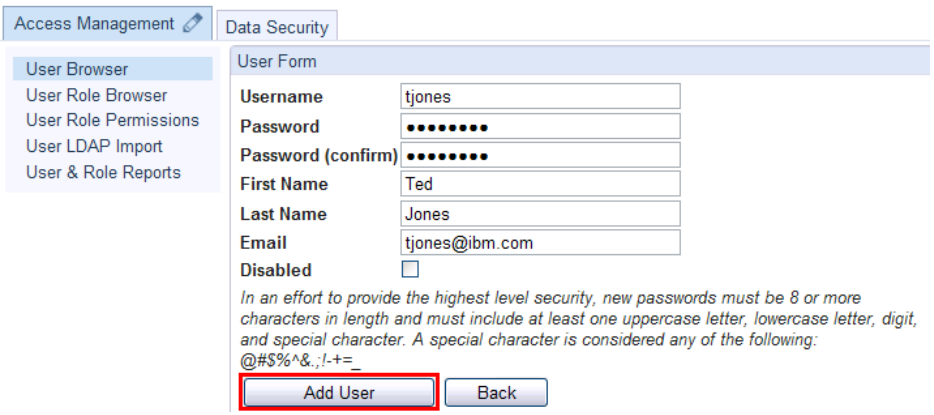
Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser - adding a user (2 of 2)

- User information includes :
  - Username - First Name - Disabled (uncheck)
  - Password - Last Name
  - Password (confirm) - Email
- All fields are required *except* email address
- The new user is added to the user role by default



© Copyright IBM Corporation 2011, 2013

Figure 4-7. User Browser - adding a user (2 of 2) GU2022.0

Notes:

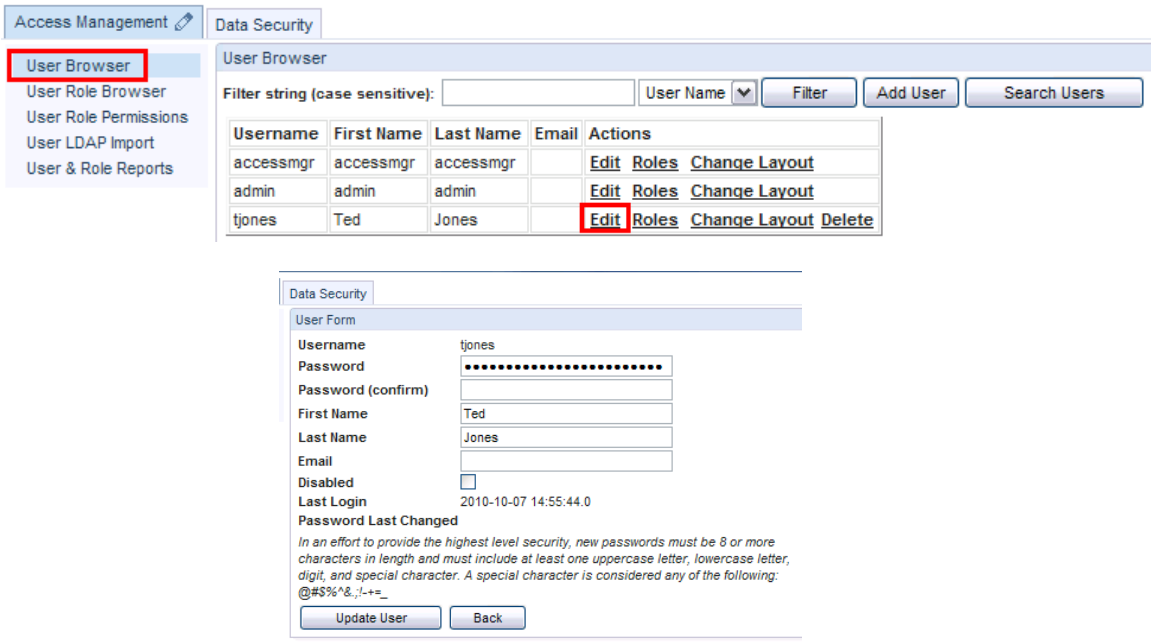
Each user has a username, password, first name, last name, and email address. Users can be enabled or disabled; be sure to uncheck the DISABLED box if you want the user to become immediately active. All users are automatically added to the **user** role by default.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser – editing a user

- The **Edit** link is used to update an existing user.
- Any attribute can be changed **except** user name.



© Copyright IBM Corporation 2011, 2013

Figure 4-8. User Browser - editing a user GU2022.0

Notes:

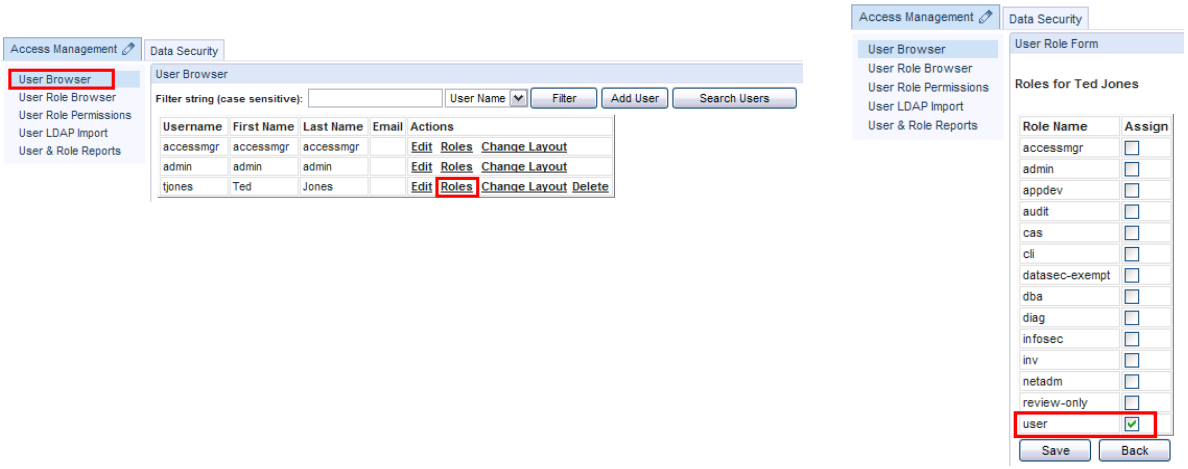
All of the settings on an existing user can be modified except for the username.

To modify an existing user, select User Browser and then click on EDIT next to the user to be modified. If the list of users is too long, you can narrow it down by using a FILTER, which includes a filter string and the field to which it applies (username, email address, etc).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser – modifying roles

- The **Roles** link is used to modify a user's role membership.
- The user becomes a member of any role that is checked.
- The user does not become a member of any role that is unchecked.



© Copyright IBM Corporation 2011, 2013

Figure 4-9. User Browser - modifying roles GU2022.0

Notes:

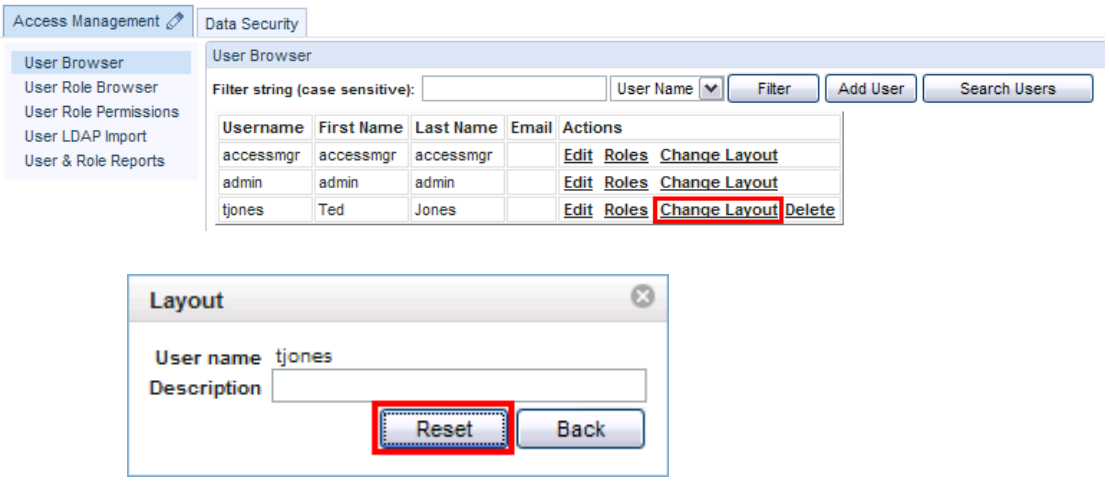
The Access Management tab is also used to assign users to roles. A user must belong to at least one of the following roles: **accessmgr**, **admin**, or **user**. By default, every new user is added to the **user** role.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser – changing layouts

- The **Change Layout** link is used to update the user's GUI to reflect modified roles.
- A user's GUI layout is determined by the roles to which the account belongs when logging into the system.



© Copyright IBM Corporation 2011, 2013

Figure 4-10. User Browser - changing layouts GU2022.0

Notes:

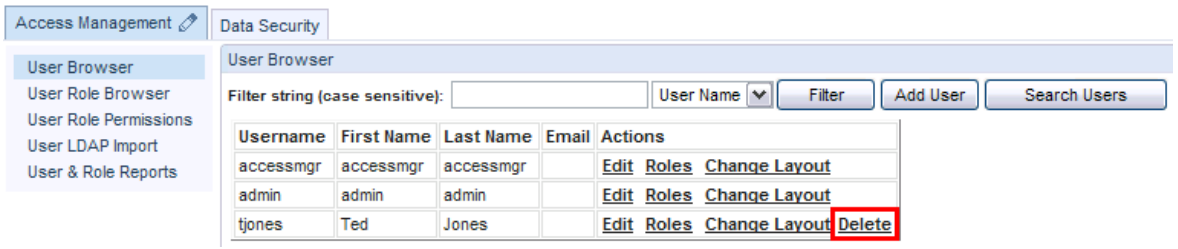
The Access Management tab is used to modify a user's GUI layout.

The user's initial GUI layout will be determined by the roles to which he/she belongs when he/she first logs into the system. For example, if a user account is assigned to accessmgr role, when logging in to the appliance for the first time, that user will only have the 'Access Management' and 'Data Security' tabs. If the admin role is later added to that user, the GUI tabs for admin will not appear until the 'Change Layout' option is selected.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Browser – deleting a user

- The **Delete** link is used to delete a Guardium user account.
- Accessmgr and admin are required users and **cannot** be deleted.



© Copyright IBM Corporation 2011, 2013

Figure 4-11. User Browser - deleting a user GU2022.0

Notes:

All objects (queries, policies, etc.) owned by a user will be reassigned to the **admin** user whenever the owning user is deleted.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User Role Browser

- A role is a group of Guardium users, all of whom have the same access privileges.
- There are several pre-defined, out-of-the box roles.
- Users can be members of roles. Roles can be assigned to items (for example, a query).
- Only members of that role can access that item.
- Custom (site specific) roles can be added or deleted by name.

© Copyright IBM Corporation 2011, 2013

Figure 4-12. User Role Browser GU2022.0

Notes:

A role is a group of Guardium users, all of whom have the same access privileges.

Default Roles

There are several pre-defined, out-of-the box roles which should never be deleted. These default roles include:

1. **user** - Provides the default layout and access for all common users.
2. **admin** - Provides the default layout and access for Guardium administrators.
3. **accessmgr** Provides the default layout and access for the access manager
4. **cli** - Provides access to CLI. The admin user has default access to CLI.
5. **diag** - See the topic, diag CLI Command in the on-line help, on how to manage the diag role.
6. **inv** - Provides the default layout and access for investigation users.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

7. **datasec-exempt**. This role is activated when Data level security is enabled. If the user has this role, a "Show-all" check box will appear in all reports.
8. **review-only** - A user specified by this role can only view results (Audit, Assessment, Classifier), Audit Results and the To Do List.

Note: A user must belong to at least one of these roles: user, admin, or accessmgr.

Sample roles

There are several sample roles that are provided out-of-the-box. They can be deleted if not needed, and include: dba, infosec, netadm, appdev, and audit.

Module –based roles

These roles will be available if the system license includes the associated software function:

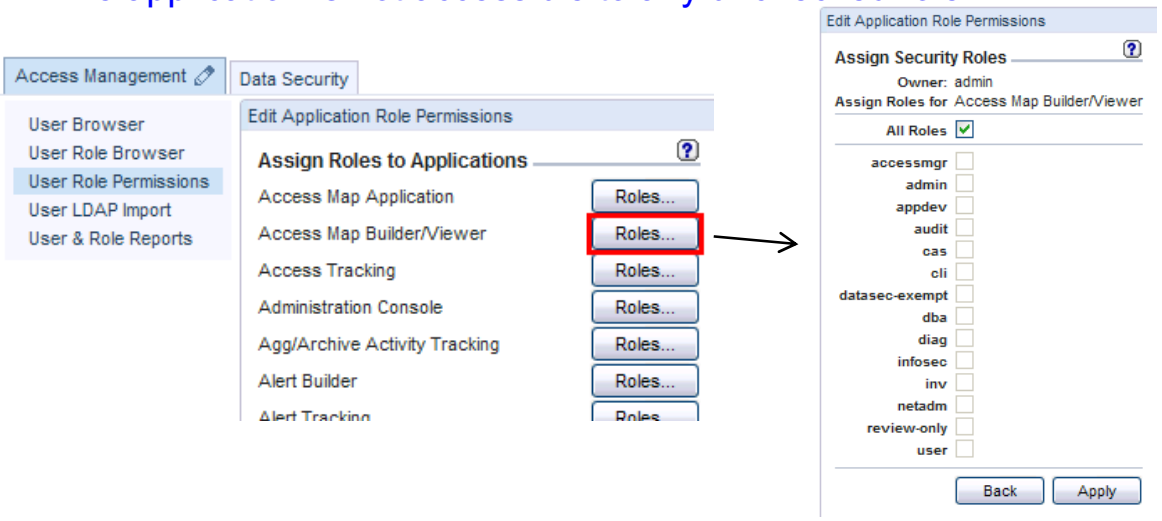
- **cas** - Configuration Auditing System (CAS)
- **pci** - Database Activity Monitor - PCI Solution Kit
- **sox** - Database Activity Monitor - SOX Solution Kit

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

User Role Permissions

- Access to each application within Guardium (that is, each Guardium function) is determined by privileges based on roles.
- Roles assigned to an application can be modified.
  - The application is accessible to each checked role.
  - The application is not accessible to any unchecked role.



© Copyright IBM Corporation 2011, 2013

Figure 4-13. User Role Permissions GU2022.0

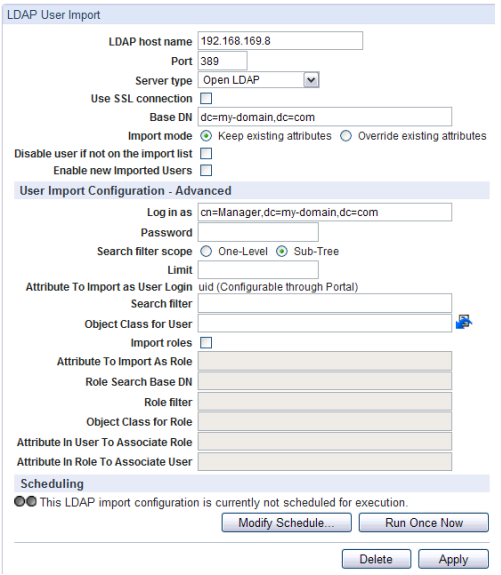
Notes:

Access to each application (that is, each Guardium function) is determined by privileges based on roles. Roles can be assigned to an application by checking the box; roles can be unassigned from an application by removing the check mark. Some applications have **All Roles** assigned. You may find that you need to uncheck the **All Roles** box and apply the individual roles as appropriate.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User LDAP Import

- User definitions can be imported from LDAP / Active Directory.



© Copyright IBM Corporation 2011, 2013

Figure 4-14. User LDAP Import GU2022.0

Notes:

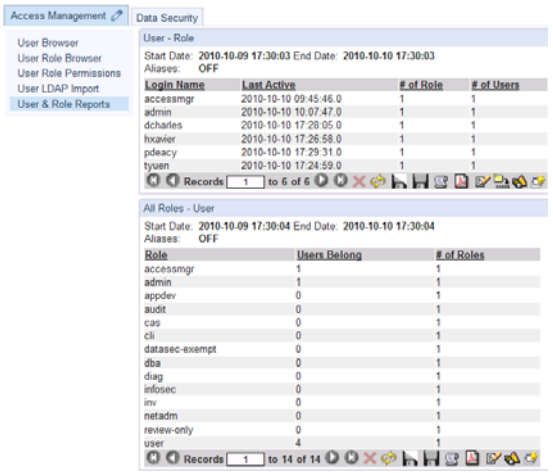
User definitions can be imported from an LDAP/Active Directory server

- To import from an LDAP server, press the **User LDAP Import** link
- Enter the required fields to access to LDAP server
- Press **Apply** and **Run Once Now**
- Choose the users to be imported. Optionally, the import process can be scheduled to run periodically or at a later date / time.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

User & Role Reports

- User & Role Reports includes access to two pre-defined reports:
  - User - Role : Lists all users with the number of roles to which each belongs. Drill-down lists the actual roles.
  - All Roles – User : Lists all roles with the number of users belonging to each role. Drill-down lists the actual users.


Access Management
Data Security
User Browser
User Role Browser
User Role Permissions
User LDAP Import
User & Role Reports
User - Role
Start Date: 2010-10-09 17:30:03 End Date: 2010-10-10 17:30:03
Aliases: OFF
Login Name | Last Active | # of Role | # of Users
accessmgr 2010-10-10 09:45:46.0 1 1
admin 2010-10-10 10:07:47.0 1 1
dcharles 2010-10-10 17:28:05.0 1 1
hxavier 2010-10-10 17:26:58.0 1 1
pdeacy 2010-10-10 17:29:31.0 1 1
tyuen 2010-10-10 17:24:59.0 1 1
Records 1 to 6 of 6
All Roles - User
Start Date: 2010-10-09 17:30:04 End Date: 2010-10-10 17:30:04
Aliases: OFF
Role | Users Belong | # of Roles
accessmgr 1 1
admin 1 1
appdev 0 1
audit 0 1
cas 0 1
cli 0 1
datasec-exempt 0 1
dba 0 1
diag 0 1
infosec 0 1
inv 0 1
netadm 0 1
review-only 0 1
user 4 1
Records 1 to 14 of 14

© Copyright IBM Corporation 2011, 2013

Figure 4-15. User & Role Reports GU2022.0

Notes:

The **User & Role Reports** link contains two reports:

- **User – Role**

Lists all users with the number of roles to which each belongs. Drill-down lists the actual roles. To access the drill down, double click any user and choose Record Details.

- **All Roles – User**

Lists all roles with the number of users belonging to each role. Drill-down lists the actual users. To access the drill-down, double click on any role and choose Record Details.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Security tab

- **Data Security** enables data level security at the observed data level, and includes:
  - Datasources Associated
  - Datasources Not Associated
  - Servers Associated
  - Servers Not Associated
  - User Heirarchy
  - User DB Association

© Copyright IBM Corporation 2011, 2013

Figure 4-16. Data Security tab GU2022.0

Notes:

- **Data Security** is designed to enable data level security at the observed data level.
  - In the case where specific Guardium users are responsible for specific databases, this mechanism will filter results system-wide so that the specific users will only be able to see the information from the specific databases for which they are responsible.
  - This would be commonly used when you have multiple business units sharing the same Guardium infrastructure but require data to be segregated between each unit.
  - This is advanced functionality and will not be covered in this training.
  - For more information, see the Access Management help book, which is accessible from the online help.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. True or False? You can delete the accessmgr user if you do not want to use it.

2. True or False? By default, new users are automatically enabled.

3. User01 is currently in the USER role, and is logged into the Guardium web interface. You add User01 to the DBA role. When will the user have access to the DBA functions?
   a. Immediately
   b. Only after logging out and logging back in
   c. Only after you run “change layout”
   d. Only after you run “change layout” and the user logs out and logs back in again

© Copyright IBM Corporation 2011, 2013

Figure 4-17. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. True or **False**? You can delete the accessmgr user if you do not want to use it.
2. True or **False**? By default, new users are automatically enabled.
3. User01 is currently in the USER role, and is logged into the Guardium web interface. You add User01 to the DBA role. When will the user have access to the DBA functions?
   a. Immediately
   b. Only after logging out and logging back in
   c. Only after you run “change layout”
   d. **Only after you run “change layout” and the user logs out and logs back in again**

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (2 of 2)

4. True or false? A Guardium user can belong to multiple roles.

5. True or false? Once set, the user name (that is, user id) cannot be changed.

6. What feature can be implemented using the Data Security tab?
   a. Assigning a user to a role
   b. Assigning an application to a role
   c. Filtering results so specific users will only be able to see information from specific databases
   d. Filtering results so specific panes will only be visible to specific users

© Copyright IBM Corporation 2011, 2013

Figure 4-18. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

4. **True** or false? A Guardium user can belong to multiple roles.
5. **True** or false? Once set, the user name (that is, user id) cannot be changed.
6. What feature can be implemented using the Data Security tab?
   a. Assigning a user to a role
   b. Assigning an application to a role
   c. **Filtering results so specific users will only be able to see information from specific databases**
   d. Filtering results so specific panes will only be visible to specific users

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Create new users
- Assign roles to new users

© Copyright IBM Corporation 2011, 2013

Figure 4-19. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 2** in the Exercise Guide.

© Copyright IBM Corporation 2012, 2013

Figure 4-20. Exercise GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (1 of 2)

1. True or **False**? You can delete the accessmgr user if you do not want to use it.

2. True or **False**? By default, new users are automatically enabled.

3. User01 is currently in the USER role, and is logged into the Guardium web interface. You add User01 to the DBA role. When will the user have access to the DBA functions?
   a. Immediately
   b. Only after logging out and logging back in
   c. Only after you run “change layout”
   d. Only after you run “change layout” and the user logs out and logs back in again

© Copyright IBM Corporation 2011, 2013

Figure 4-21. Checkpoint solution (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (2 of 2)

4. **True** or false? A Guardium user can belong to multiple roles.

5. **True** or false? Once set, the user name (that is, user id) cannot be changed.

6. What feature can be implemented using the Data Security tab?
   a. Assigning a user to a role
   b. Assigning an application to a role
   c. Filtering results so specific users will only be able to see information from specific databases
   d. Filtering results so specific panes will only be visible to specific users

© Copyright IBM Corporation 2011, 2013

Figure 4-22. Checkpoint solution (2 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 5. System View and Administration Console I

Estimated time

00:45

What this unit is about

This unit describes how to use the administration console to configure a Guardium appliance.

What you should be able to do

After completing this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

© Copyright IBM Corporation 2011, 2013

Figure 5-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

System View

- Default tab for admin users
- Includes:
  - S-TAP Status Monitor
  - Current Status Monitor
  - Request Rate
  - CPU Usage
  - Logins to Guardium
  - Scheduled Job Exceptions

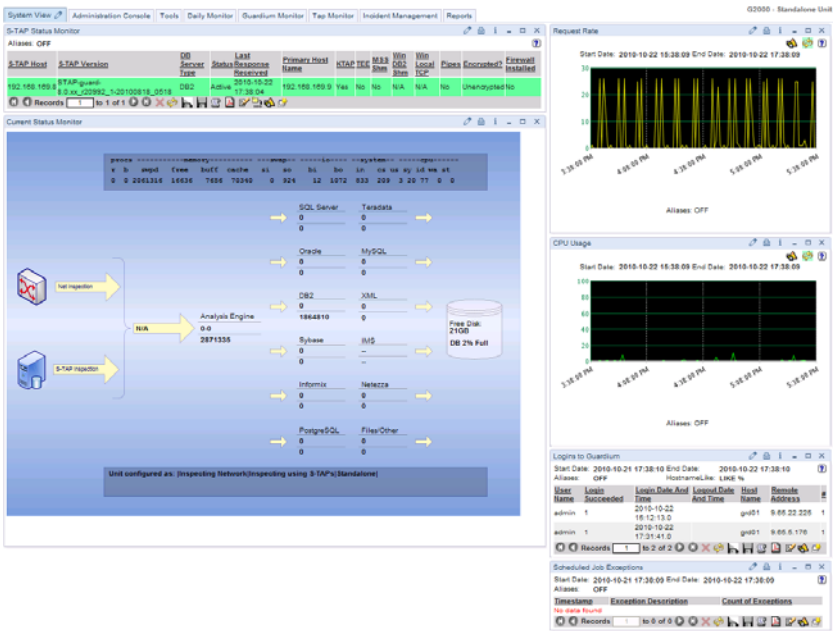


Figure 5-2. System View GU2022.0

Notes:

System View is the default tab that is displayed whenever the admin User, or any user in the admin role, logs into the Guardium Console web interface. System View provides a dashboard of the appliance's current state, and includes the following:

- **S-TAP Status Monitor** – The S-TAP Status Monitor area shows a report listing each of the S-TAPs directed to this appliance, along with its current status. Green indicates an inspection engine has been configured and is running for the S-TAP.
- **Current Status Monitor** – The Current Status Monitor area includes a graphic that displays key system information, such as the number of requests logged and free disk space. Notice the numbers indicating a DB2 instance is being monitored.
- **Request Rate** – The Request Rate area shows is a chart highlighting the number SQL requests logged over a period of time.
- **CPU Usage** – The CPU Usage area is a a chart displaying CPU utilization over a period of time.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

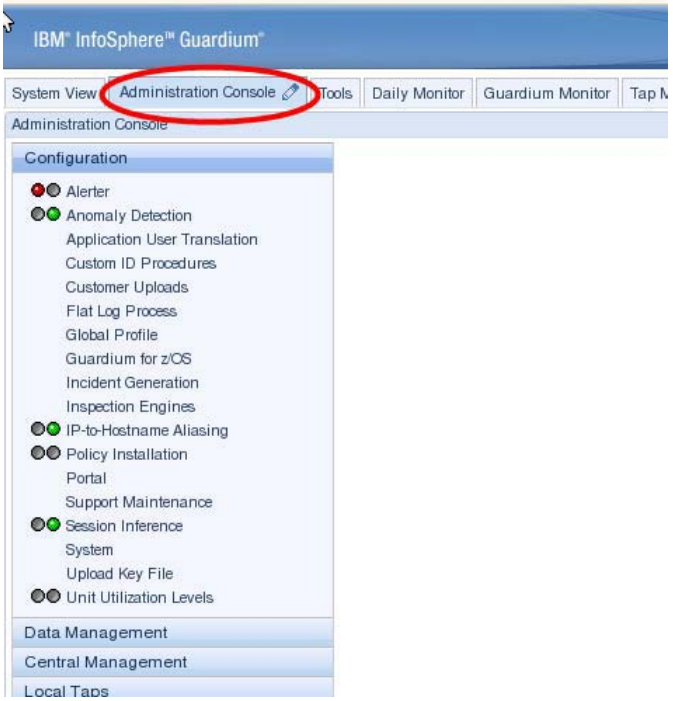
- **Logins to Guardium –** The Logins to Guardium area shows a report of recent logins to the Guardium appliance.
- **Scheduled Job Exceptions** – The Scheduled Job Exceptions area includes a report listing any recent issues with scheduled jobs.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Administration Console

- The Administration Console includes:
  - Configuration
  - Data Management
  - Central Management
  - Local Taps
  - Guardium Definitions
  - Custom Classes
  - Module Installation



© Copyright IBM Corporation 2011, 2013

Figure 5-3. Administration Console GU2022.0

Notes:

The Administration Console tab is the starting point for many activities performed by admin (or users in the admin role). It includes:

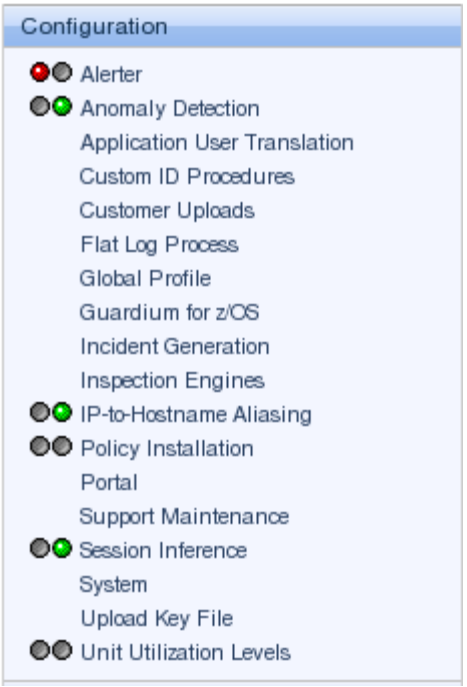
- **Configuration**
- **Data Management**
- **Central Management**
- **Local Taps**
- **Guardium Definitions**
- **Custom Classes**
- **Module Installation**

In this module, we will look at the Configuration options.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Administration Console - Configuration

- Configuration options
  - Alerter
  - Anomoly Detection
  - Application User Translation
  - Custom ID Procedures
  - Customer Uploads
  - Flat Log Process
  - Global Profile
  - Guardium for z/OS
  - Incident Generation
  - Inspection Engines
  - IP-to-Hostname Aliasing
  - Policy Installation
  - Portal
  - Support Maintenance
  - Session Inference
  - System
  - Upload Key File
  - Unit Utilization Levels



© Copyright IBM Corporation 2011, 2013

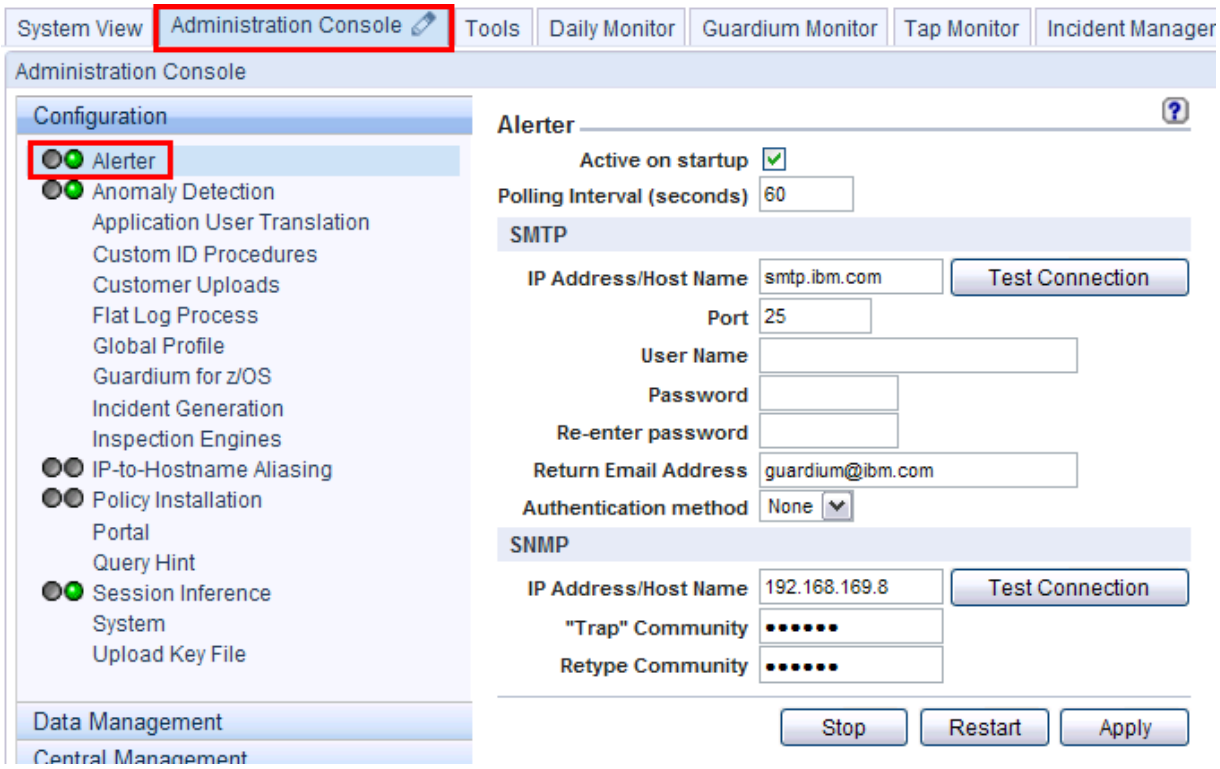
Figure 5-4. Administration Console - Configuration GU2022.0

Notes:

The Administration Console pane includes a link to the Configuration options. We will look at each of the options on the upcoming pages.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration – Alerter



© Copyright IBM Corporation 2011, 2013

Figure 5-5. Configuration - Alerter GU2022.0

Notes:

The Alerter enables the use of email messages, SNMP traps, and alert related Syslog messages. No e-mail messages, SNMP traps, or alert related Syslog messages will be sent until the Alerter is configured and activated. Other components create and queue messages for the Alerter. The Alerter checks for and sends messages based on the polling interval that has been configured for it.

Active on startup

If marked the Alerter will be activated automatically each time the appliance restarts.

Polling

Sets the frequency that the Alerter checks for and sends messages. The polling interval is measured in seconds. This should usually be left at the default frequency, which is every 60 seconds.

SMTP

The SMTP section is used to configure the Alerter to send SMTP (email) messages. You can configure the SMTP connections as follows:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

IP Address / **Host Name**: Enter the IP address or hostname for the SMTP gateway.

Port: Enter the SMTP port number. It is usually set to port 25.

Test Connection (Optional) Click the **Test Connection** button to verify the SMTP address and port. This only tests that there is access to specified host and port. It does not verify that this is a working SMTP server. A dialog box is displayed, informing you of the success or failure of the operation.

User Name: If your SMTP server uses authentication, enter a valid user name for your mail server.

Password: Enter the password for the above user if your SMTP server uses authentication. Re-enter it in the Re-enter Password box.

Return E-mail Address: Enter the return address for e-mail sent by the system. This address is usually an administrative account that is checked often.

Authentication Method: Select AUTH if your SMTP server uses authentication. Otherwise, select **None**. When Auth is selected, you must specify the user name and password to be used for authentication.

Click the **Apply** button to save the configuration.

Click **Restart** to restart the Alerter with the new configuration.

Note: The Alerter will not begin using a new configuration until it is restarted.

The **SNMP** section of the Configuration pane is used to configure the Alerter to send SNMP traps. You can configure the SNMP connections as follows:

- **IP Address**: Enter the IP address/hostname to which the SNMP trap will be sent.
- **Test Connection (**Optional): Click the Test Connection button to verify the SNMP address and port (22). This only tests that there is access to specified host and port. It does not verify that this is a working SNMP server. A dialog box is displayed, informing you of the success or failure of the operation.
- **Trap" Community**: Enter the community name for the trap. Retype the community in the **Retype Community** box.

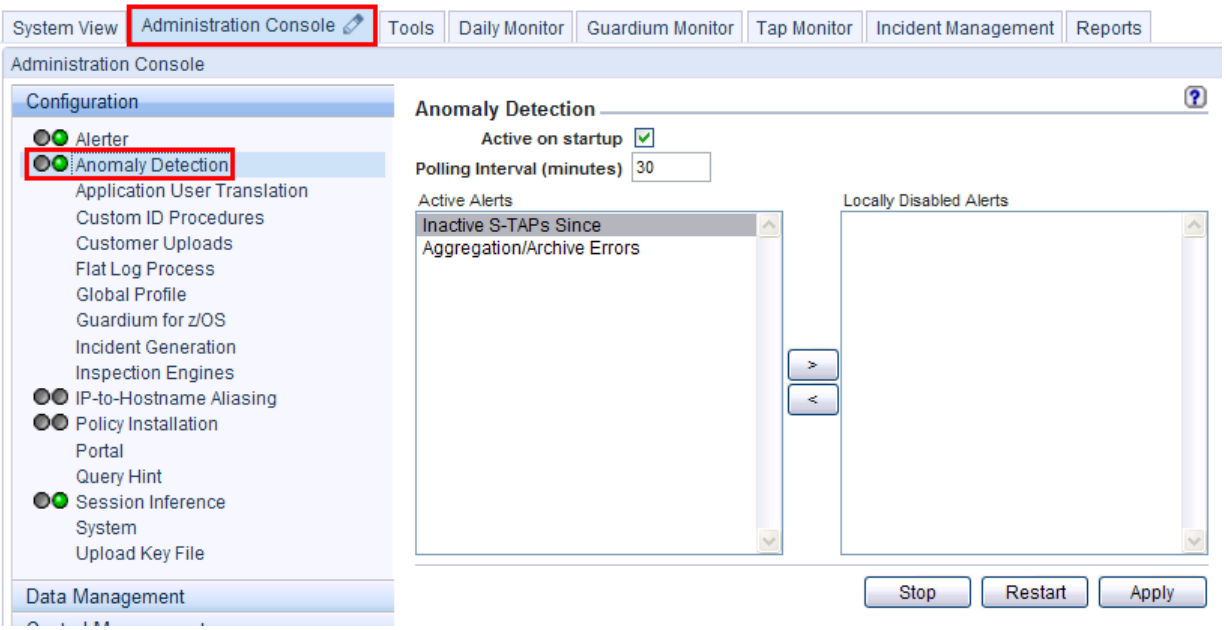
- Click the **Apply** button to save the configuration.
- Click **Restart** to restart the Alerter with the new configuration.

Note: The Alerter will not begin using a new SNMP configuration until it is restarted.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Anomaly Detection



© Copyright IBM Corporation 2011, 2013

Figure 5-6. Configuration - Anomaly Detection GU2022.0

Notes:

The Anomaly Detection process executes **correlation alerts** according to the schedule defined for each alert. A *correlation alert* looks back over a specified period of time to determine if a condition has been satisfied (for example, an excessive number of failed logins for a single user).

In a Central Manager environment, the Anomaly Detection panel is used to turn off correlation alerts that are not appropriate for a particular appliance. Under Central Management, all correlation alerts are defined on the Central Manager, and when activated, will be activated on all appliances by default.

Anomaly Detection options include:

Active on startup checkbox - automatically starts Anomaly Detection on startup.

Polling Interval sets the frequency that Anomaly Detection checks for appliance issues. This should not be changed without consulting with Guardium support because increasing the frequency can cause performance issues.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

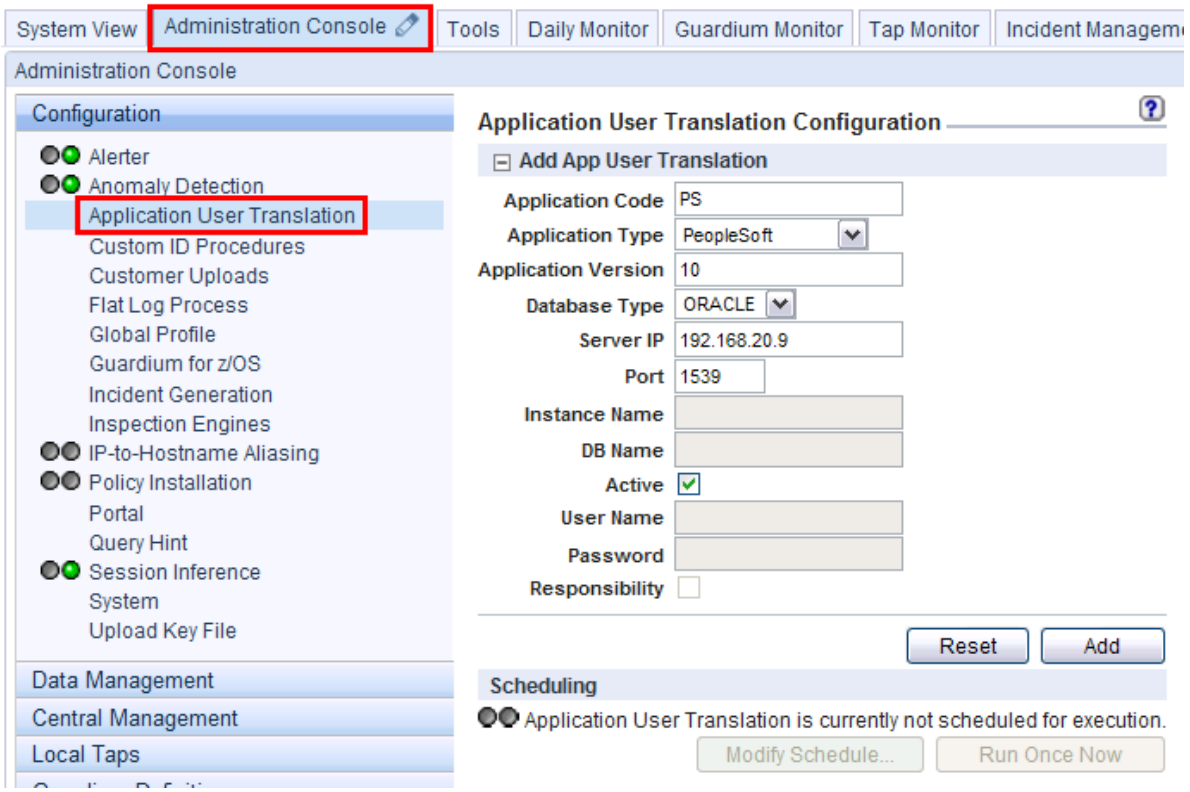
The **Active Alerts** allows you to enable or disable Active Alerts. To disable an alert globally in a Central Manager environment, it will be easier to clear the **Active** checkbox from the alert itself. To enable or disable an alert on a single appliance in a Central Management environment, follow the procedure outlined below:

- To disable an alert, select it from the **Active Alerts** box, and click **Disable**.
- To enable an alert, select it from the **Locally Disabled Alerts** box, and click **Enable**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Configuration - Application User Translation



© Copyright IBM Corporation 2011, 2013

Figure 5-7. Configuration - Application User Translation GU2022.0

Notes:

Some applications manage a pool of database connections. In such three-tier architectures, the pooled connections all log into a database using a single functional ID, and then manage all application users internally. When a user session needs access to the database, it acquires a connection from the pool, uses it, and then releases it back to the pool. When this happens, Guardium can see how the application interacts with the database, but it cannot attribute specific database actions to specific application users. For some widely used applications (such as SAP and PeopleSoft), Guardium has built-in support for identifying the end-user information from the application, and can therefore relate database activity to the application end-users.

Applications supported by ‘Application User Translation’ include:

- BO-WI - Business Objects / Web Intelligence
- EBS - Oracle E-Business Suite
- PeopleSoft
- SAP Observed

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- SAP DB
- SIEBEL Observed
- SIEBEL DB

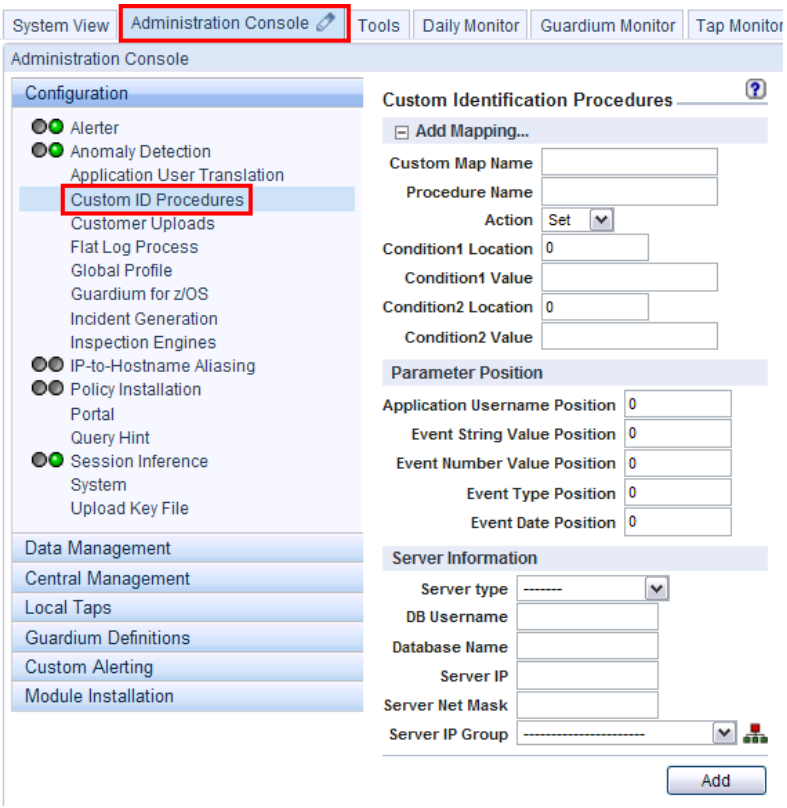
If you need to log the application user for an application not included in the above list, the following options provide alternate methods to achieving the same results:

- Identify Users via API, see the on-line help
- Identify Users via Stored Procedures, see the next page

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Configuration - Custom ID Procedures



© Copyright IBM Corporation 2011, 2013

Figure 5-8. Configuration - Custom ID Procedures GU2022.0

Notes:

In many existing applications, all of the information needed to identify an application user can be obtained from existing database traffic using stored procedure calls. Once Guardium knows what calls to watch for, and which parameters contain the user name or other information of interest, users can be identified automatically.

In the simplest case, an application might have a single stored procedure that sets a number of property values, one of which is the user name. A call to set the user name might look like this:

Using BO-WI - Business Objects / Web Intelligence

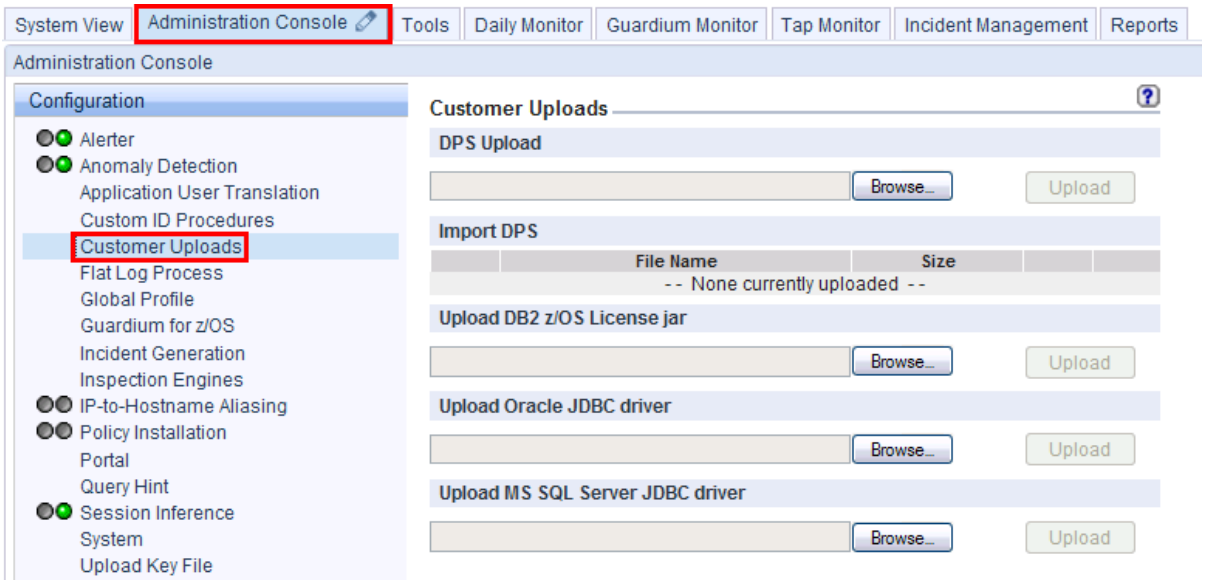
```
set_application_property('user_name', 'JohnDoe');
```

In a custom procedure mapping (described later), you can tell Guardium to:

- Watch for a stored procedure named *set_application_property*, with a first parameter value of *user_name*.
- Set the application user to the value of the second parameter in the call (*JohnDoe*, in the example above).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Customer Uploads



© Copyright IBM Corporation 2011, 2013

Figure 5-9. Configuration - Customer Uploads GU2022.0

Notes:

Database Activity Monitor Content Subscription (previously known as Database Protection Subscription Service) supports the maintenance of predefined assessment tests, SQL based tests, CVEs, and groups such as database versions and patches. DPS is provided as a service to keep information current and within industry best practices to protect against newly discovered vulnerabilities. Distribution of updates will be done on a quarterly basis. Uploading Jar files is also done through at this menu screen.

Note: If a custom group exists with the same name as a predefined Guardium group, the upload process will add "Guardium - " in front of the name for the predefined group.

- Select Administration Console > **Customer Uploads**
- For **DPS Upload -** Enter the name of the file to be uploaded or click the Browse button to locate and select that file.
- **Import DPS** identifies what files have been uploaded.
- For **Upload DB2 z/OS License jar** - Enter the name of the file to be uploaded or click the Browse button to locate and select that file.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

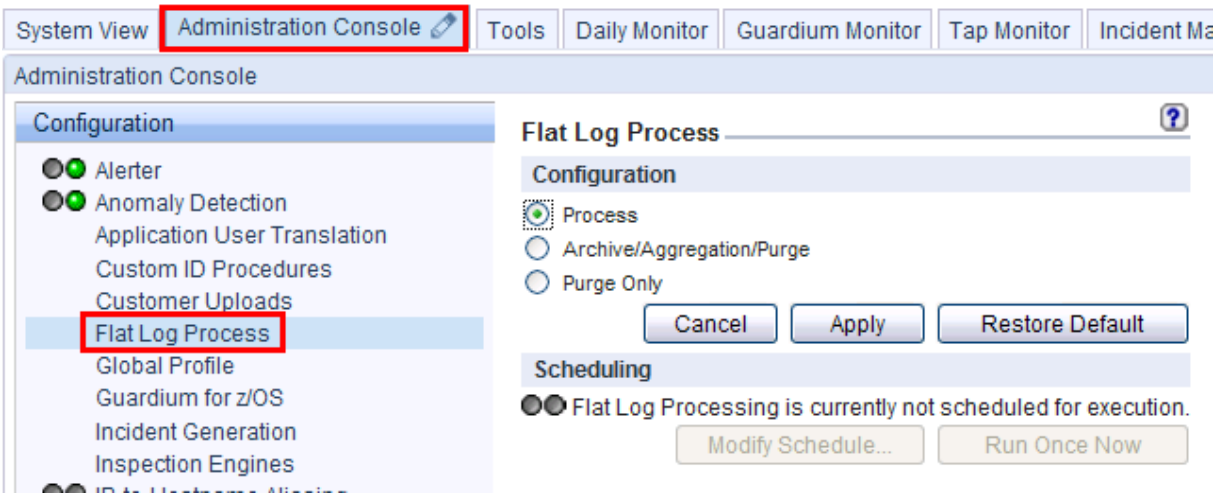
- For **Upload Oracle JDBC driver**, or **Upload MS SQL Server JDBC driver** - Use this function to upload open source drivers for Oracle and MS SQL. Oracle Data Direct and MS SQL Data Direct drivers are pre-loaded in the Guardium appliance. Use this function to upload open source drivers for Oracle and MS SQL which will appear, after upload, in the Database Type drop-down menu in Datasources Definition menu. Upload one driver at a time.
- Click the **Upload** button. You are notified when the operation completes, and the file uploaded will be displayed. This action brings the uploaded file to Central Manager. For the Oracle JDBC and SQL Server JDBC driver files, go to Central Management choice within Admin Console to manage distribution of these Jar file to the managed units.
- Click to import or click to remove the uploaded file without importing.
- You will be prompted to confirm either action.
- Click the **Done** button when finished.

Note: If you will be exporting and importing definitions from one appliance to another, be aware that subscribed groups are not exported. When exporting definitions that reference subscribed groups, you must ensure that all referenced subscribed groups are installed on the importing appliance (or central manager in a federated environment).

Note: When uploading DB2 z/OS License jar files, the license will take effect after restart of the GUI.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Flat Log Process



© Copyright IBM Corporation 2011, 2013

Figure 5-10. Configuration - Flat Log Process GU2022.0

Notes:

The Flat Log option is a process to allow the Guardium appliance to log information without immediately parsing it in real-time. This saves processing resources, so that a heavier traffic volume can be handled. The parsing and amalgamation of that data to Guardium's internal database can be done later, either on a collector or an aggregator unit.

Note: Rules on flat files do not work with policy rules involving a field, an object, SQL verb (command), Object/Command Group, and Object/Field Group. In the Flat Log process, "flat" means that a syntax tree is not built. If there is no syntax tree, then the fields, objects and SQL verbs cannot be determined.

The following actions do not work with rules on flat policies: LOG_FULL_DETAILS; LOG_FULL_DETAILS_PER_SESSION; LOG_FULL_DETAILS_VALUES; LOG_FULL_DETAILS_VALUES_PER_SESSION; LOG_MASKED_DETAILS.

When **Log Flat (Flat Log)** checkbox option listed in **Policy Definition** screen of **Policy Builder** is checked

- Data will not be parsed in real-time

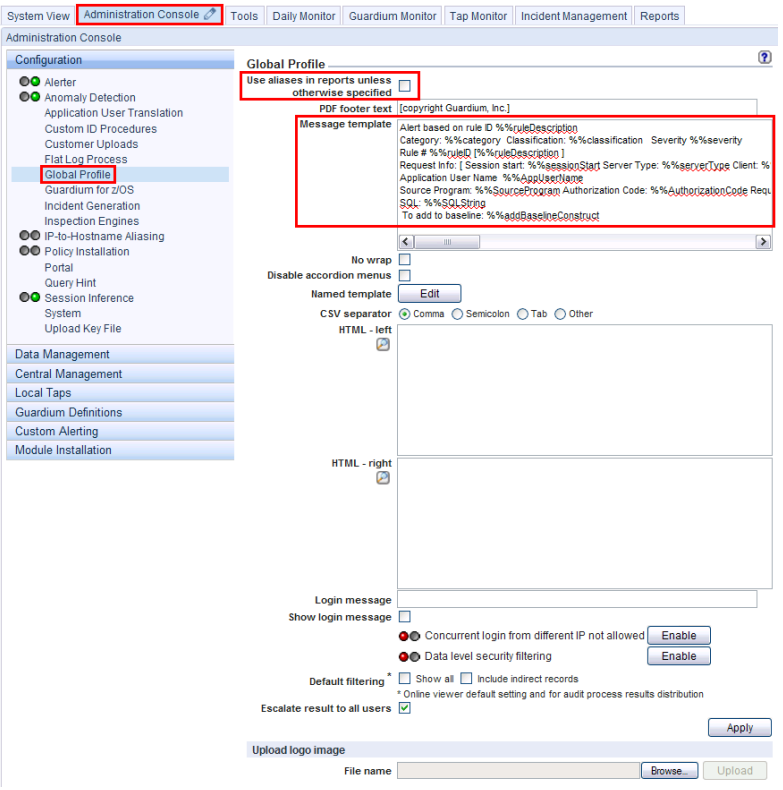
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- The flat logs can be seen on a designated Flat Log List report
- The offline process to parse the data and merge to the standard access domains is configured through the **Administration Console.**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Global Profile



© Copyright IBM Corporation 2011, 2013

Figure 5-11. Configuration - Global Profile GU2022.0

Notes:

The Global Profile panel defines defaults that apply to all users.

Below are details on each of the options contained within this screen. Note, 'Use Aliases in Reports unless otherwise specified' and 'Message template' are the most commonly accessed settings.

- **Use Aliases in Reports unless otherwise specified** – allows you to display aliases by default on all reports. This is especially helpful with displaying hostnames instead of IP addresses.
- The **PDF Footer Text** changes the text displayed at the bottom of each page for each PDF document generated by the appliance.
- **Message Template** customizes the message format used to generate alerts. Note, this is often changed to enable SIEM integration.
- The **No wrap** checkbox below allows you to see where the line breaks appear in the message.

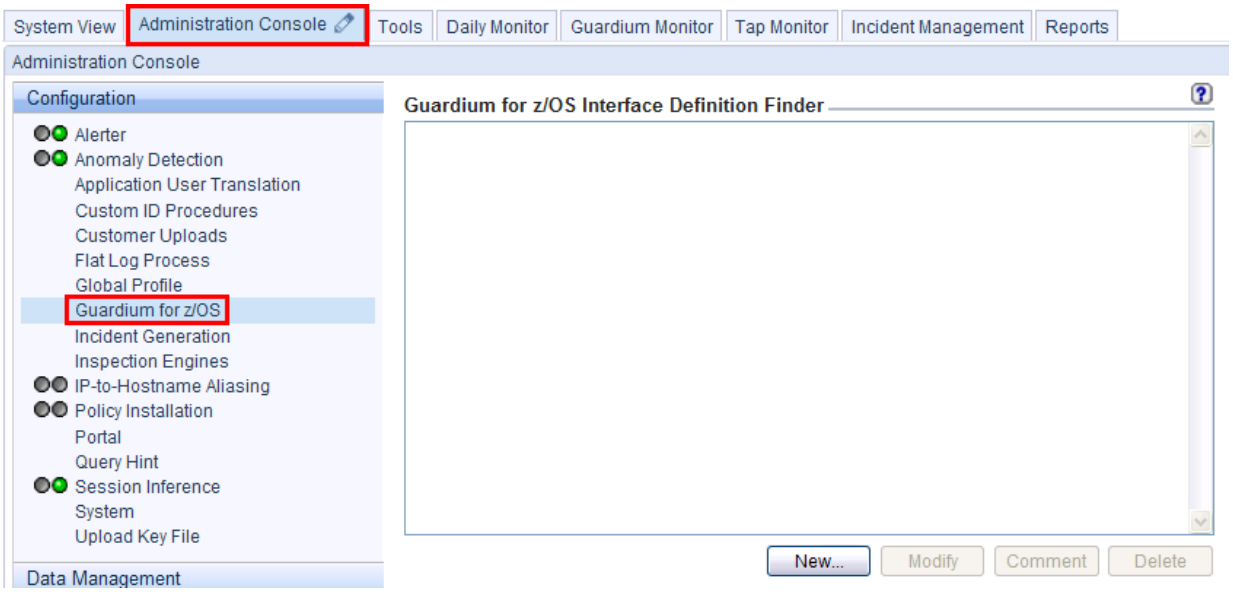
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **No accordion menus** - Check this box to display the Tools tab with Config and Control and Report Building in one column and their associated functions in another column.
- **Named template** - The feature defines multiple message templates and facilitates the use of different templates on different rules. In the past, only a single message template was available for all rules, all receiver types, etc.
- **CVS Separator** – defines a separator to be used in audit processes
- **HTML – left** / **right** allows you to change the text displayed at the top of the page
- **Login message** / **Show login message** – displays a pop-up message to users upon login
- **Concurrent login from different IP not allowed –** when enabled, each Guardium user will be allowed to log in from only one IP address at a time.
- **Data level security filtering** – when enabled, the system will filter results, system-wide, in a way that each user will only be able to see the information from those databases that the user is responsible for.
  - **Default filtering -** Permits the logged-in viewer to see all the rows in the result regardless of who these rows belong to. When used with the *Datasec-exempt* role permits an override of the data level security filtering.
  - **Include indirect records** - Permits the logged-in viewer to see the rows that belong to the logged-in user, but also all rows that belong to users below the logged-in user in the user hierarchy.
- **Escalate result to all users** - A check mark in this check box escalates audit process results (and PDF versions) to all users, even if data level security at the observed data level is enabled.
- **Upload logo image** - adds a company logo graphic to the upper right portion of the Guardium window

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Guardium for z/OS



© Copyright IBM Corporation 2011, 2013

Figure 5-12. Configuration - Guardium for z/OS GU2022.0

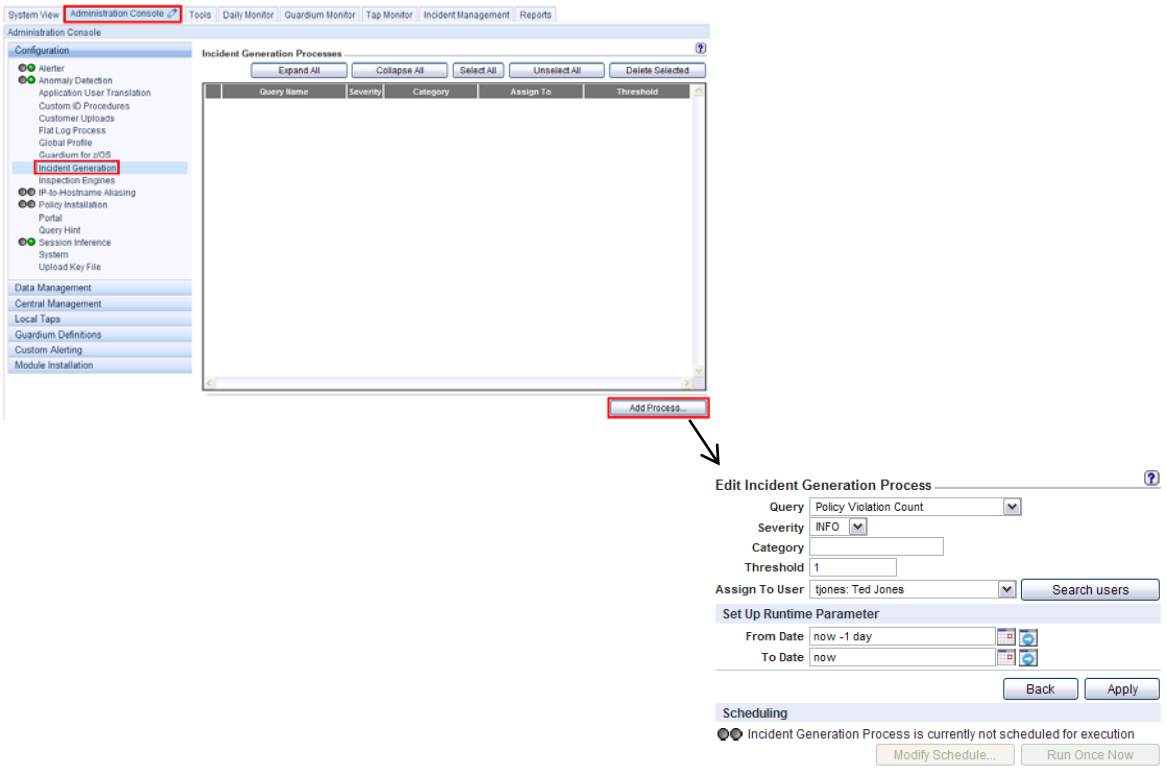
Notes:

This screen is used to configure Guardium to monitor traffic from DB2 on z/OS.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Incident Generation Process



© Copyright IBM Corporation 2011, 2013

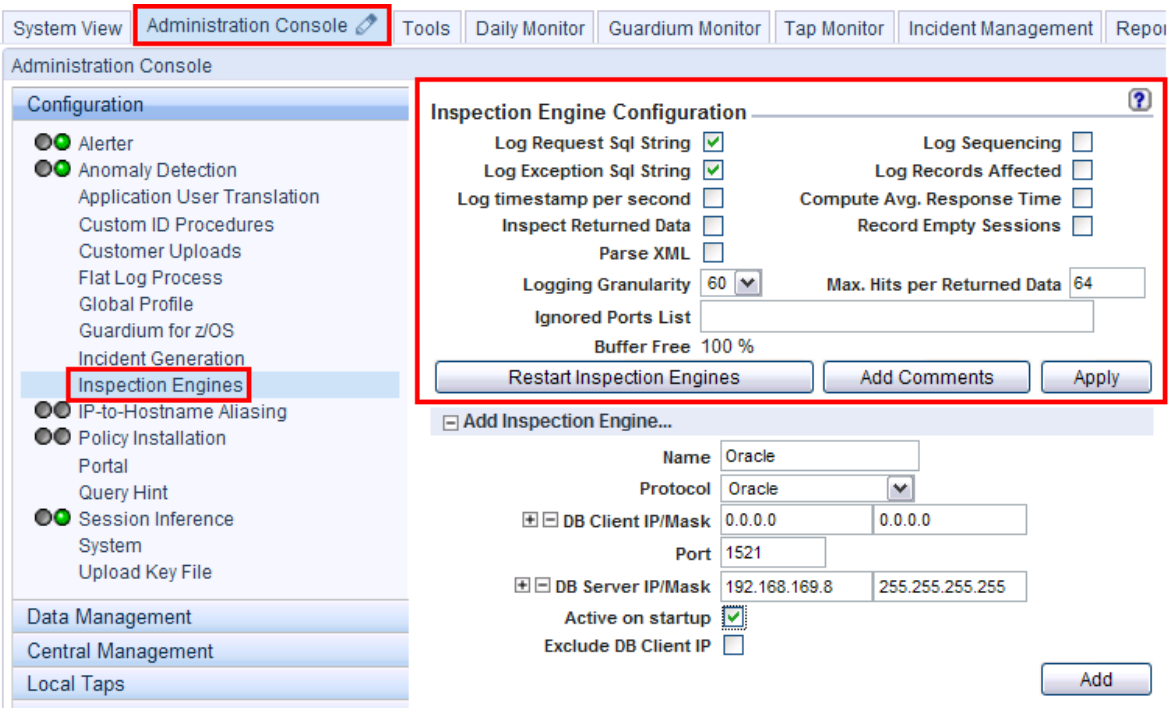
Figure 5-13. Configuration - Incident Generation Process GU2022.0

Notes:

The Integrated Incident Management (IIM) application provides a business-user interface with workflow automation for tracking and resolving database security incidents. It simplifies incident management by allowing administrators to group a series of related policy violations into a single incident and assign them to specific individuals. This reduces the number of separate policy violations that oversight teams need to review.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Inspection Engines (1 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 5-14. Configuration - Inspection Engines (1 of 2) GU2022.0

Notes:

Inspection Engine Configuration controls settings that apply to all inspection engines

- **Log Request Sql String** - If marked, each SQL request statement is logged in its sanitized format. Otherwise, no statements are logged.
- **Log Sequencing** - If marked, a record is made of the immediately previous SQL statement, as well as the current SQL statement, provided that the previous construct occurs within a short enough time period.
- **Log Exception Sql String** - If marked, when exceptions are logged, the entire SQL statement is logged.
- **Log Records Affected** - If marked, the number of records affected is recorded for each SQL statement (when applicable) as well as the ingress and egress counts. Note: When using JDBC, this must be marked to properly log Oracle bind variable traffic
- **Log timestamp per second** - If marked, allows you to display the distribution of requests down to the second, regardless of the default logging granularity (see below).

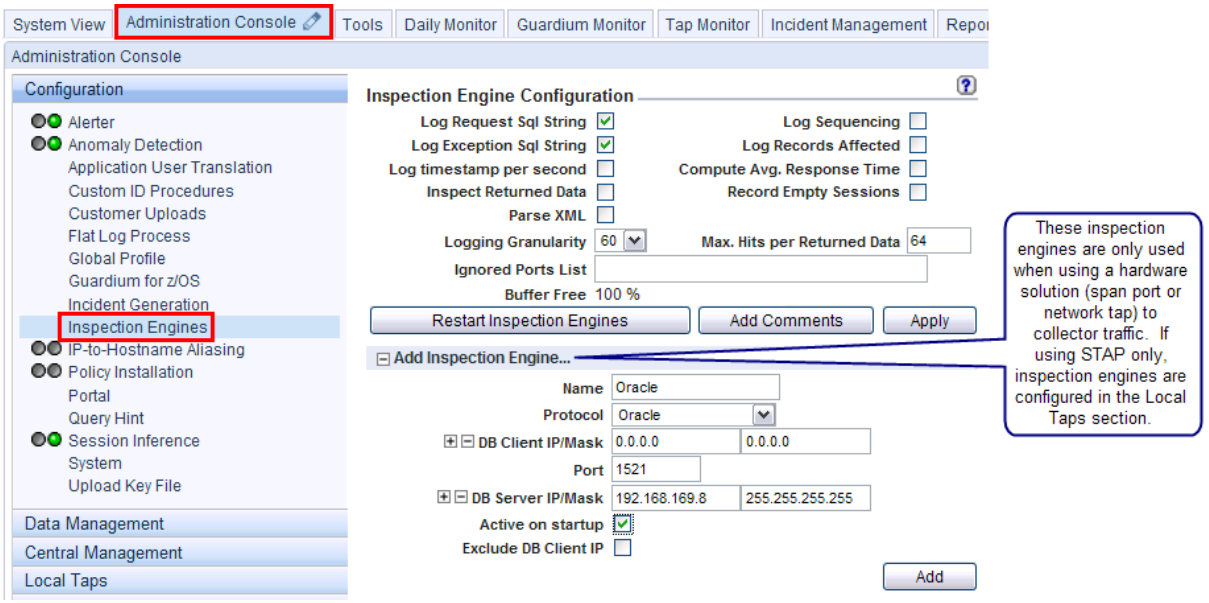
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Logging Granularity** - The number of minutes (1, 2, 5, 10, 15, 30, or 60) in a logging unit. If requested in a report, Guardium summarizes request data at this granularity. For example, if the logging granularity is 60, a certain request occurred n times in a given hour. If the above check box is not marked, exactly when the command occurred within the hour is not recorded. But, if a rule in a policy is triggered by a request, a real time alert can indicate the exact time. When you define exception rules for a policy, those rules can also apply to the logging unit. For example, you might want to ignore 5 login failures per hour, but send an alert on the sixth login failure.
- **Inspect Returned Data** - Mark to inspect data returned by SQL requests. If *extrusion* rules will be used in the security policy, this checkbox must be marked.
- **Max. Hits per Returned Data** - When returned data is being inspected, indicate how many hits (policy rule violations) are to be recorded.
- **Compute Avg Response Time** - When marked, for each SQL construct logged, the average response time will be computed.
- **Record Empty Sessions** - When marked, sessions containing no SQL statements will be logged. When cleared, these sessions will be ignored.
- **Buffer Free**: n % - Display only. **n** is the percent of free buffer space available for the inspection engine process. This value is updated each time the window is refreshed. There is a single inspection engine process that drives all inspection engines. This is the buffer used by that process.
- **Ignored Ports List** - A list of ports to be ignored. Add values to this list if you know your database servers are processing non-database protocols, and you want Guardium to not waste cycles analyzing non-database traffic. For example, if you know the host on which your database resides also runs an HTTP server on port 80, you can add 80 to the ignored ports list, ensuring that Guardium will not process these streams. Separate multiple values with commas, and use a hyphen to specify an inclusive range of ports. For example: 101,105,110-223
- **Restart Inspection Engines** - Click the Restart Inspection Engines button to stop and restart all inspection engines.
- **Comment** - Click the Comment button to add comments to the Inspection Engine Configuration.
- **Apply** - Click the Apply button to save the configuration.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Inspection Engines (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 5-15. Configuration - Inspection Engines (2 of 2) GU2022.0

Notes:

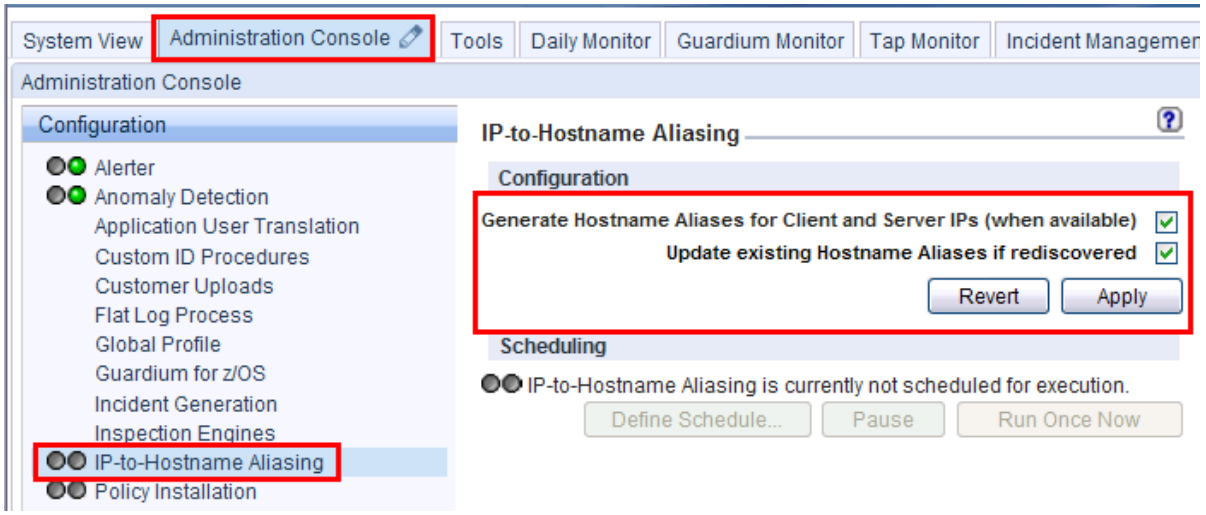
Inspection Engine Configuration – Add Inspection Engine (for SPAN port or Network Taps only)

An **inspection engine** monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example). The inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - IP-to-Hostname Aliasing



© Copyright IBM Corporation 2011, 2013

Figure 5-16. Configuration - IP-to-Hostname Aliasing GU2022.0

Notes:

The **IP-to-Hostname Aliasing** function accesses the Domain Name System (DNS) server to define hostname aliases for client and server IP addresses. Note that there are two separate sets of IP addresses - one for clients, and one for servers. When IP-to-Hostname Aliasing is enabled, alias names will replace IPs within Guardium where appropriate.

- Mark the **Generate Hostname Aliases for Client and Server IPs (when available)** checkbox to enable hostname aliasing
- A second checkbox displays when the first is marked: **Update existing Hostname Aliases if rediscovered**. Mark the "Update existing..." checkbox to update a previously defined alias that does not match the current DNS hostname (usually indicating that the hostname for that IP address has changed). You may not want to do this if you have assigned some aliases manually. For example, assume that the DNS hostname for a given IP address is **dbserver204.guardium.com**, but that server is commonly known as the *QA Sybase Server*. If **QA Sybase Server** has been defined manually as an alias for that IP address, and the "Update" checkbox is marked, that alias will be overwritten by the DNS hostname.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Click the **Apply** button to save the IP-to-Hostname Aliasing configuration.

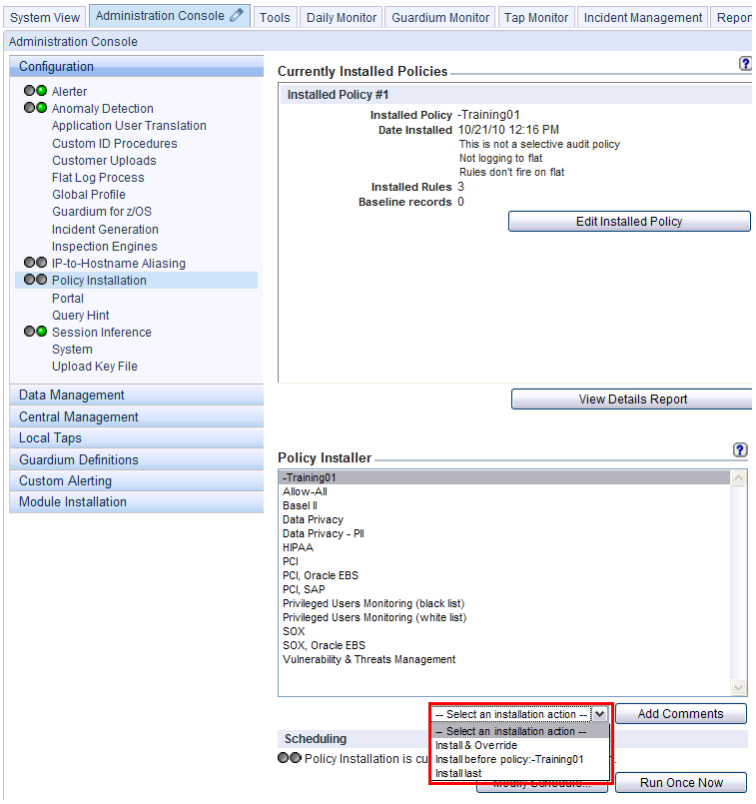
Do one of the following:

- Click the **Run Once Now** button to generate the aliases immediately
- Click the **Define Schedule** button to define a schedule for running this task.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Configuration - Policy Installation



© Copyright IBM Corporation 2011, 2013

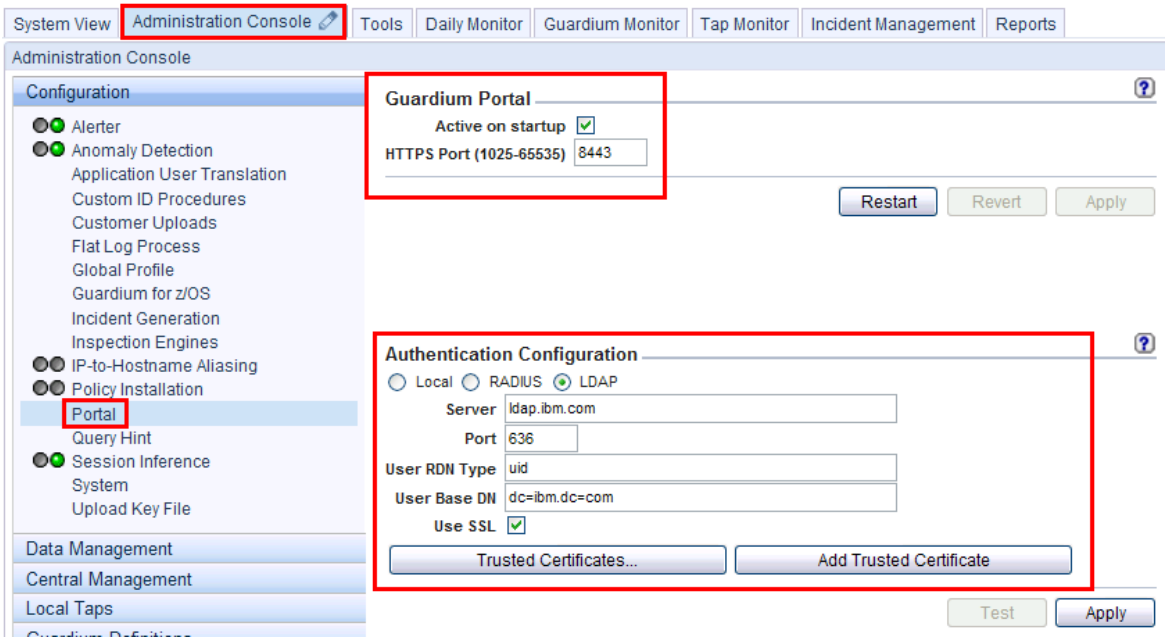
Figure 5-17. Configuration - Policy Installation GU2022.0

Notes:

Policies must be installed to take effect. This will be covered in the 'Policy' unit.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Portal



© Copyright IBM Corporation 2011, 2013

Figure 5-18. Configuration - Portal GU2022.0

Notes:

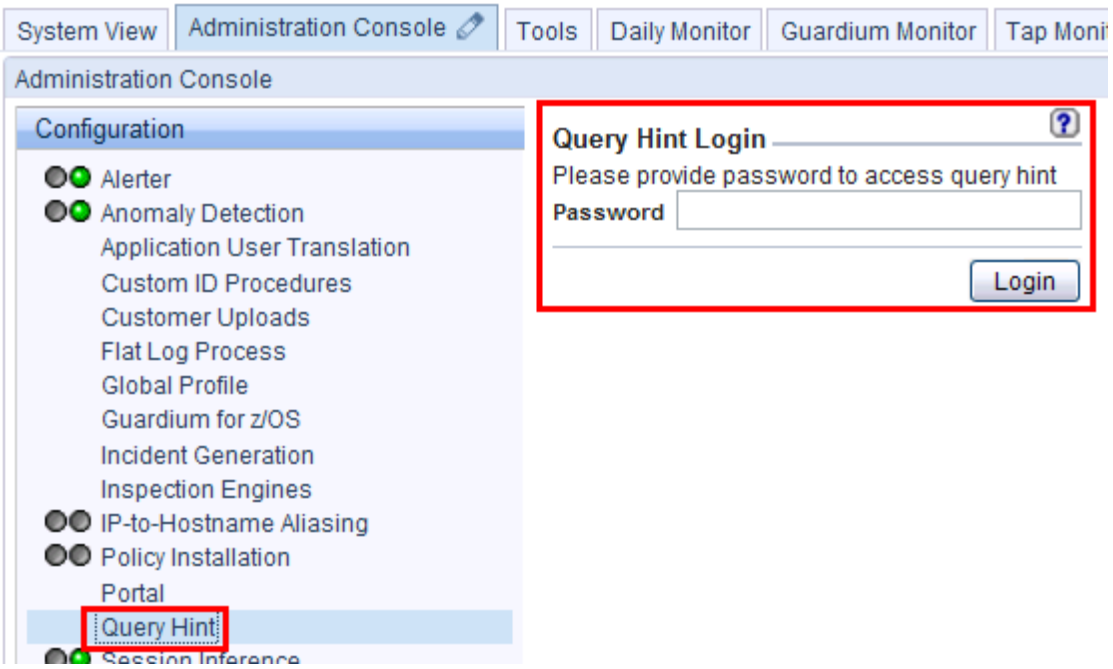
Guardium Portal - You can keep the Guardium appliance Web server on its default port (8443) or reset the portal as described below. We strongly recommend that you use the default port.

Authentication Configuration - By default, Guardium user logins are authenticated by Guardium, independent of any other application. For the Guardium *admin* user account, login is *always* authenticated by Guardium alone. For all other Guardium user accounts, authentication can be configured to use either RADIUS or LDAP. In the latter cases, additional configuration information for connecting with the authentication server is required.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Query Hint



© Copyright IBM Corporation 2011, 2013

Figure 5-19. Configuration - Query Hint GU2022.0

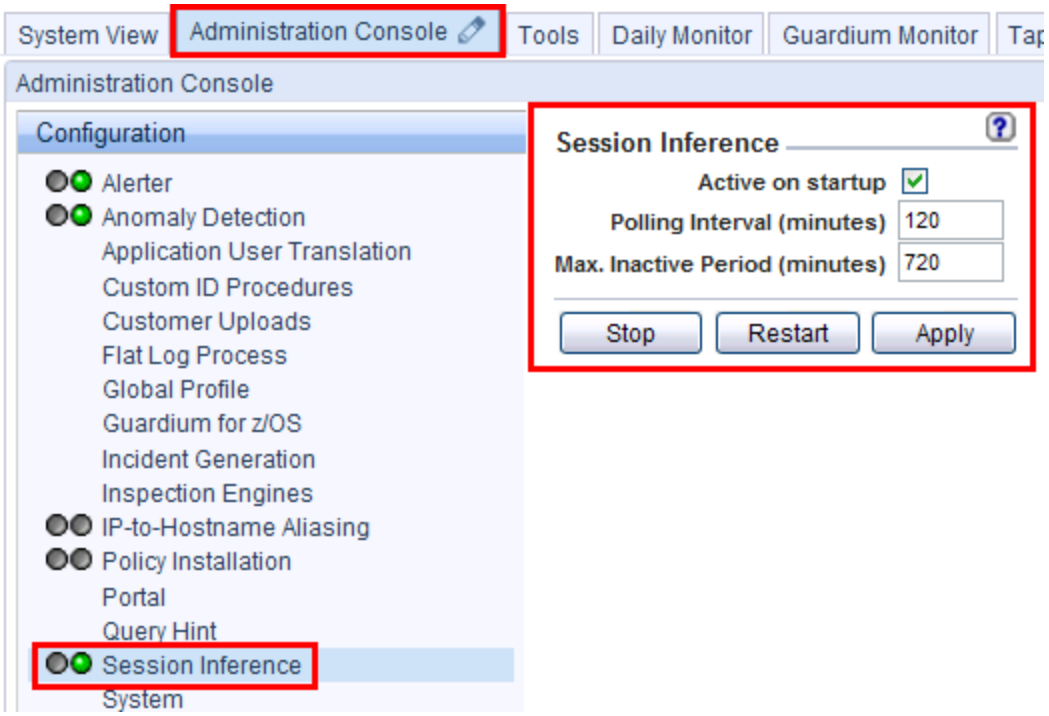
Notes:

This feature is password protected and can be used only as directed by Technical Support. Contact Technical Support if you require more information.

The Query Hint screen is also used to activate two policy log actions, "Log full details with values" and "Log full details with values per session". After filling in the Query Hint password, an additional button will appear, "Add value logging option to policies".

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - Session Inference



© Copyright IBM Corporation 2011, 2013

Figure 5-20. Configuration - Session Inference GU2022.0

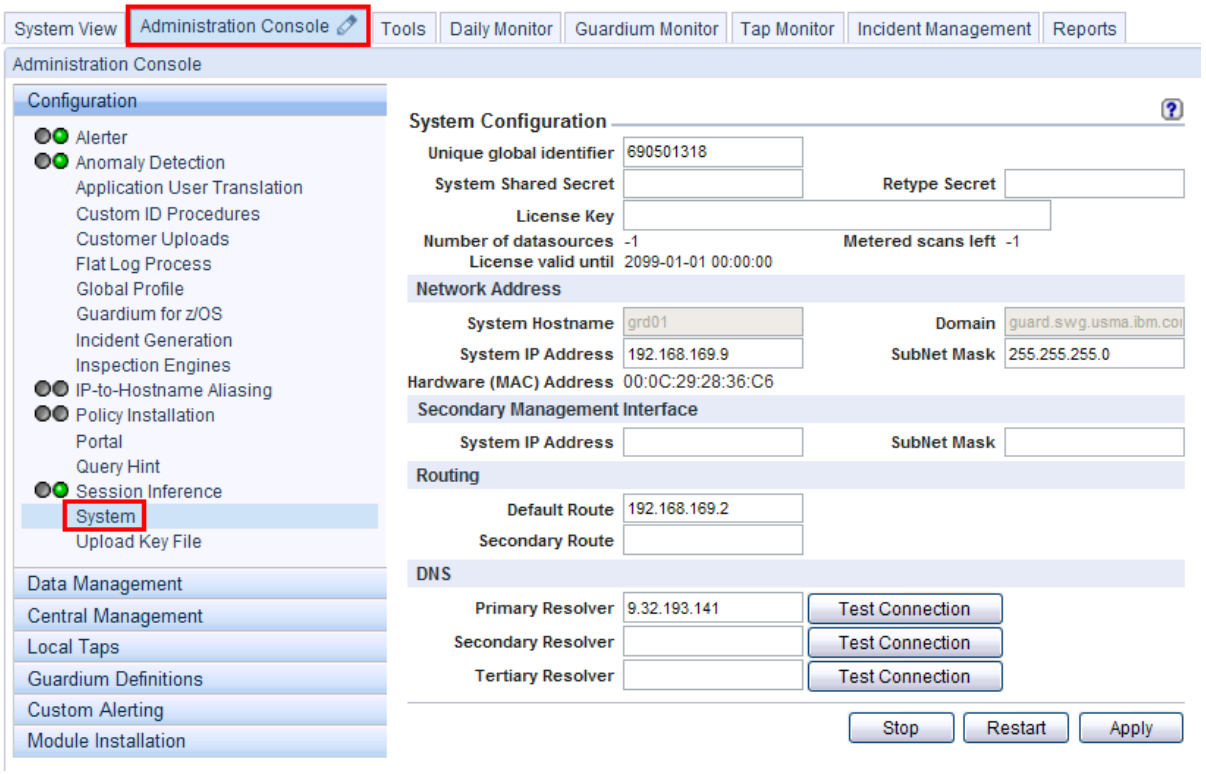
Notes:

Session Inference checks for open sessions that have not been active for a specified period of time, and marks them as closed. These settings should not be changed.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration - System



© Copyright IBM Corporation 2011, 2013

Figure 5-21. Configuration - System GU2022.0

Notes:

System Configuration

- **Unique global identifier -** This value is used for collation and aggregation of data. The default value is a unique value derived from the MAC address of the machine. It is strongly recommended that you do not change this value after the system begins monitoring operations.
- **System Shared Secret** - Any value you enter here does not display. Each character you type displays as an asterisk.
  - The system shared secret is used for archive/restore operations, and for Central Management and Aggregation operations. When used, its value must be the same for all units that will communicate. This value is null at installation time, and can change over time.
  - The system shared secret is used:
    - When secure connections are being established between a Central Manager and a managed unit.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

  - When an aggregated unit signs and encrypts data for export to the aggregator.
  - When any unit signs and encrypts data for archiving.
  - When an aggregator imports data from an aggregated unit.
  - When any unit restores archived data.
- Depending on your company's security practices, you may be required to change the system shared secret from time to time. Because the shared secret can change, each system maintains a *shared secret keys* file, containing an historical record of all shared secrets defined on that system. This allows an exported (or archived) file from a system with an older shared secret to be imported (or restored) by a system on which that same shared secret has been replaced with a newer one.
- **Caution**: When used, be sure to save the shared secret value in a safe location. If you lose the value, you will not be able to access archived data.

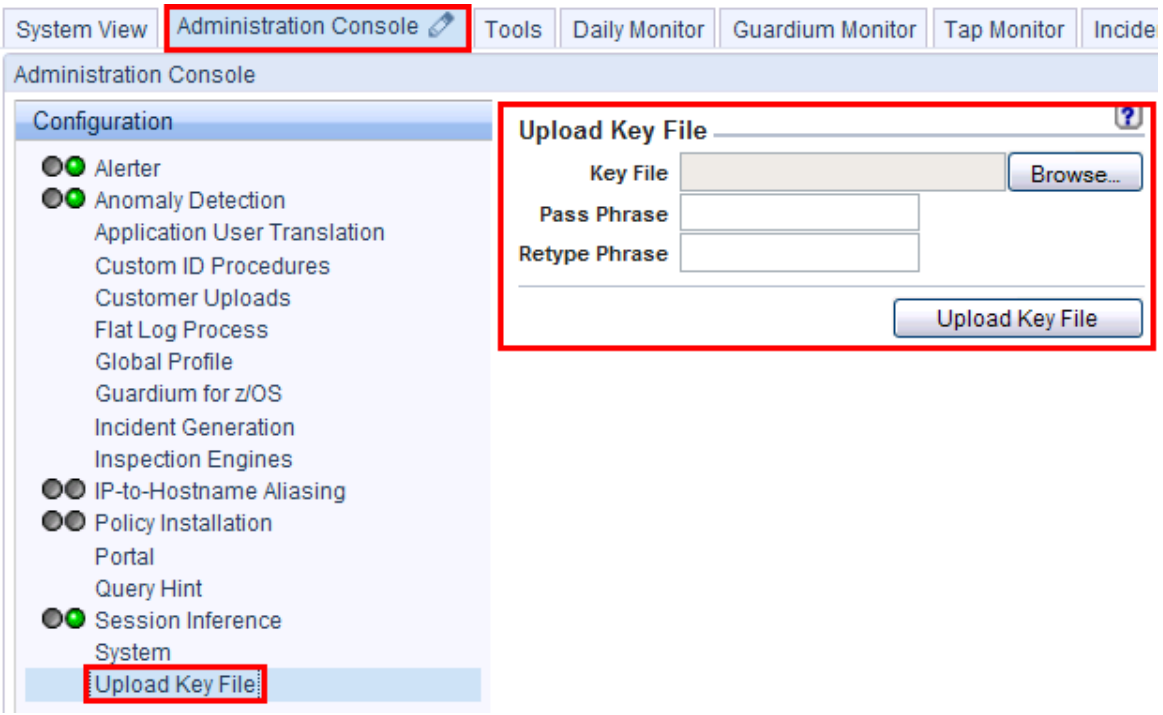
- **License Key** - This value is not displayed. It is inserted in the configuration during installation. Do not modify this field unless you are instructed to do so by Technical Support. You may need to paste a new product key here if optional components are being added.

The remaining fields allow you to change the basic network settings (IP address, default route, etc.).

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Configuration - Upload Key File



© Copyright IBM Corporation 2011, 2013

Figure 5-22. Configuration - Upload Key File GU2022.0

Notes:

Under rare conditions, a Microsoft SQL Server key file must be uploaded to the Guardium appliance, in order for the appliance to monitor encrypted SQL Server traffic. No key file is needed if an S-TAP has been installed on the SQL Server and configured to handle encryption. This is the recommended and most common way of configuring an S-TAP agent for MS SQL Server. To determine if an S-TAP is configured to handle encrypted MS SQL Server traffic

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. A(n) _____ monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol
2. Using the S-TAP Status Monitor on the System View pane, how can you tell if an inspection engine has been configured or not?
3. Which of the following is NOT a function of the Configuration option on the Administration Console?
    a. Create and configure Guardium users
    b. Create and configure Inspection engines
    c. Configure local taps
    d. Upload and install software modules
4. Appling license keys is a function of the _____ configuration option.

© Copyright IBM Corporation 2011, 2013

Figure 5-23. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

1. An **inspection engine** monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol
2. Using the S-TAP Status Monitor on the System View pane, how can you tell if an inspection engine has been configured or not?

   If it is green, an inspection engine is configured and running.
3. Which of the following is NOT a function of the Configuration option on the Administration Console?
   a. **Create and configure Guardium users**
   b. Create and configure Inspection engines
   c. Configure local taps
   d. Upload and install software modules
4. Appling license keys is a function of the **system** configuration option.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

© Copyright IBM Corporation 2011, 2013

Figure 5-24. Unit summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. A(n) **inspection engine** monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol

2. Using the S-TAP Status Monitor on the System View pane, how can you tell if an inspection engine has been configured or not? **If it is green, an inspection engine is configured and running.**

3. Which of the following is NOT a function of the Configuration option on the Administration Console?
   a. **Create and configure Guardium users**
   b. Create and configure Inspection engines
   c. Configure local taps
   d. Upload and install software modules

4. Appling license keys is a function of the **system** configuration option.

© Copyright IBM Corporation 2011, 2013

Figure 5-25. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 6. System View and Administration Console II

Estimated time

00:45

What this unit is about

This unit describes how to use the administration console for additional Guardium appliance configurations.

What you should be able to do

After completing this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

© Copyright IBM Corporation 2011, 2013

Figure 6-1. Unit objectives GU2022.0

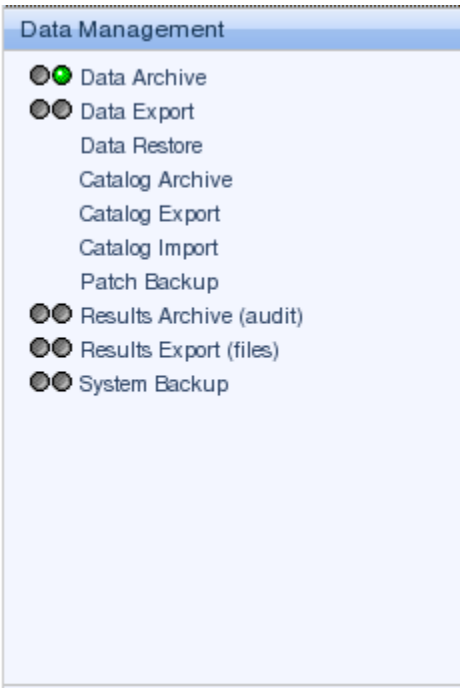
Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Administration Console - Data Management

Data Management includes

- Data Archive
- Data Export
- Data Restore
- Catalog Archive
- Catalog Export
- Catalog Import
- Patch Backup
- Results Archive (audit)
- Results Export (files)
- System Backup



© Copyright IBM Corporation 2011, 2013

Figure 6-2. Administration Console - Data Management GU2022.0

Notes:

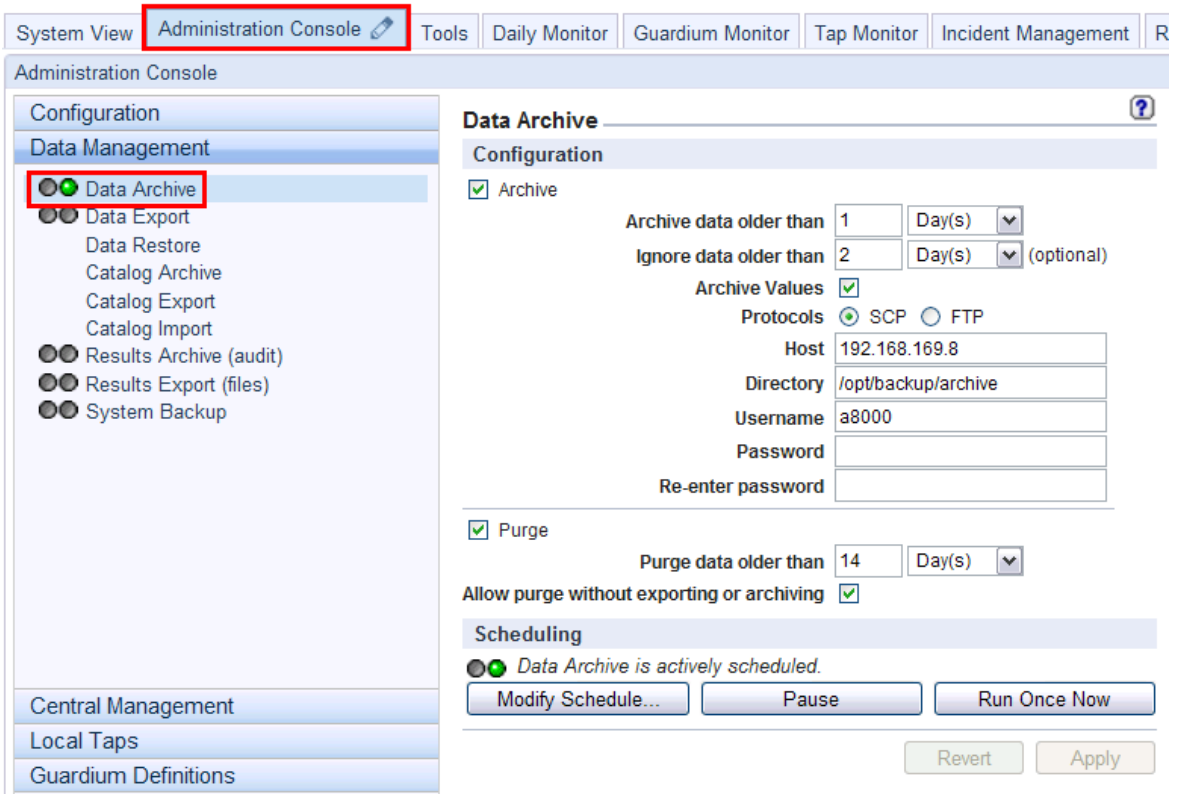
Data Management includes

- Data Archive
- Data Export
- Data Restore
- Catalog Archive
- Catalog Export
- Catalog Import
- Patch Backup
- Results Archive (audit)
- Results Export (files)
- System Backup

These feature will be discussed in the upcoming pages.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Data archive and purge



© Copyright IBM Corporation 2011, 2013

Figure 6-3. Data Management - Data archive and purge GU2022.0

Notes:

Archive and purge operations should be run on a scheduled basis. **Data Archive** backs up the data that has been captured by the appliance within a given time period. When configuring Data Archive, a purge operation can also be configured. Typically, data is archived at the end of the day on which it is captured, which ensures that in the event of a catastrophe, only the data of that day is lost. The purging of data depends on the application and is highly variable, depending on business and auditing requirements.

Typically, **Archive data older than** should be set to **1 Day** and **Ignore data older than** set to **2 days**. This will always create an archive of the previous day's data. In an environment with collectors and aggregators, it is recommended to archive from the collectors and, if backup space allows, the aggregator.

It is very important to configure the purge process. If data is not purged from the system, the database will eventually become full and logging will stop. The **Purge data older than** setting indicates the maximum number of daysthe data will be kept on the appliance. **Allow purge without exporting or archiving** controls whether the system will allow data

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

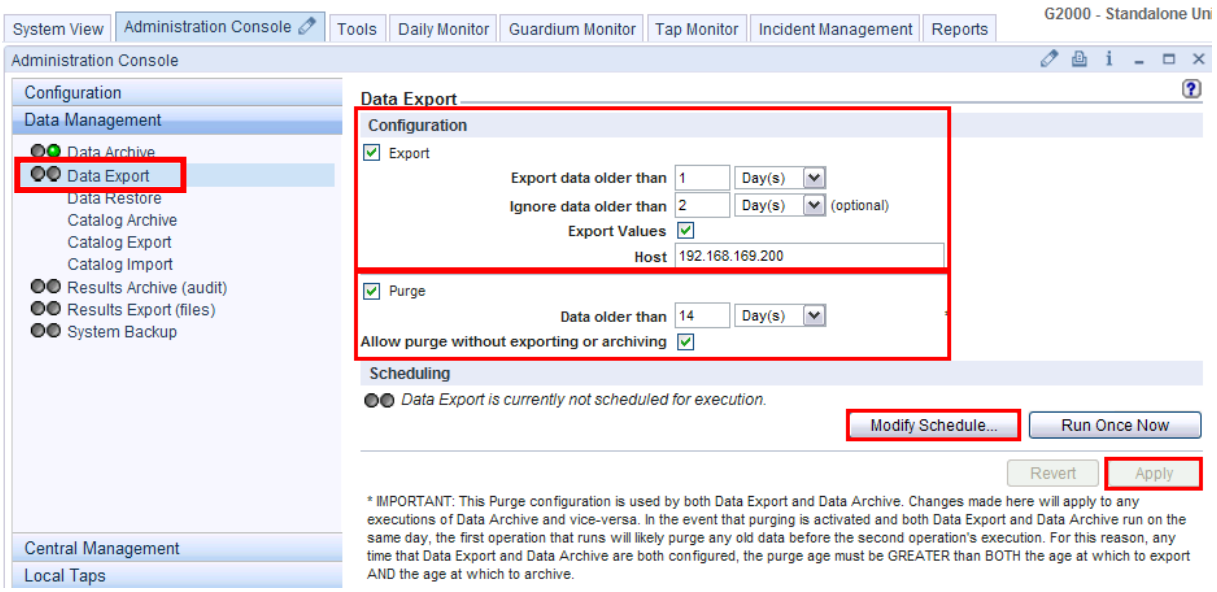
to be purged before it is archived or exported. This may be necessary if, for example, you are archiving data from your collectors but not your aggregators.

Other settings include

- **Archive Values** box to include values (from SQL strings) in the archived data. If this box is cleared, values will be replaced with question mark characters on the archive (and hence the values will not be available following a restore operation).
- **Storage method radio button** provides a value chosen from the list below. Depending on how the appliance has been configured, one or more of these buttons may not be available. For a description of how to configure the archive and backup storage methods, see the description of the **show** and **store storage-system** commands in the CLI Appendix. Available options include EMC CENTERA, TSM, SCP, and FTP
- **Host**/**Directory**/**Username**/**Password** – enter the credentials required for the destination server.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Data Export


System View
Administration Console
Tools
Daily Monitor
Guardium Monitor
Tap Monitor
Incident Management
Reports
G2000 - Standalone Uni
Administration Console
Configuration
Data Management
Data Archive
Data Export
Data Restore
Catalog Archive
Catalog Export
Catalog Import
Results Archive (audit)
Results Export (files)
System Backup
Central Management
Local Taps
Data Export
Configuration
Export
Export data older than 1 Day(s)
Ignore data older than 2 Day(s) (optional)
Export Values
Host 192.168.169.200
Purge
Data older than 14 Day(s)
Allow purge without exporting or archiving
Scheduling
Data Export is currently not scheduled for execution.
Modify Schedule...
Run Once Now
Revert
Apply
* IMPORTANT: This Purge configuration is used by both Data Export and Data Archive. Changes made here will apply to any executions of Data Archive and vice-versa. In the event that purging is activated and both Data Export and Data Archive run on the same day, the first operation that runs will likely purge any old data before the second operation's execution. For this reason, any time that Data Export and Data Archive are both configured, the purge age must be GREATER than BOTH the age at which to export AND the age at which to archive.

© Copyright IBM Corporation 2011, 2013

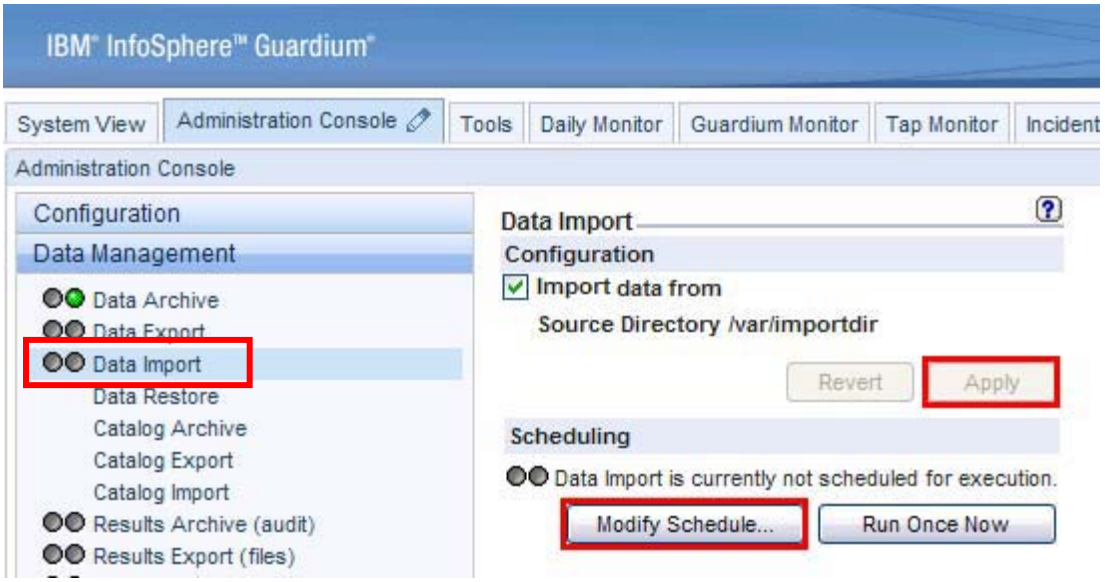
Figure 6-4. Data Management - Data Export GU2022.0

Notes:

Data Export configures the export of data from a collector to an aggregator and, like data archive, should be set to **Export data older than** *1* day and **Ignore data older than** *2* days. Note, if you change the purge parameters here, they will also be changed in the data archive screen.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Data Import (Aggregator only)



© Copyright IBM Corporation 2011, 2013

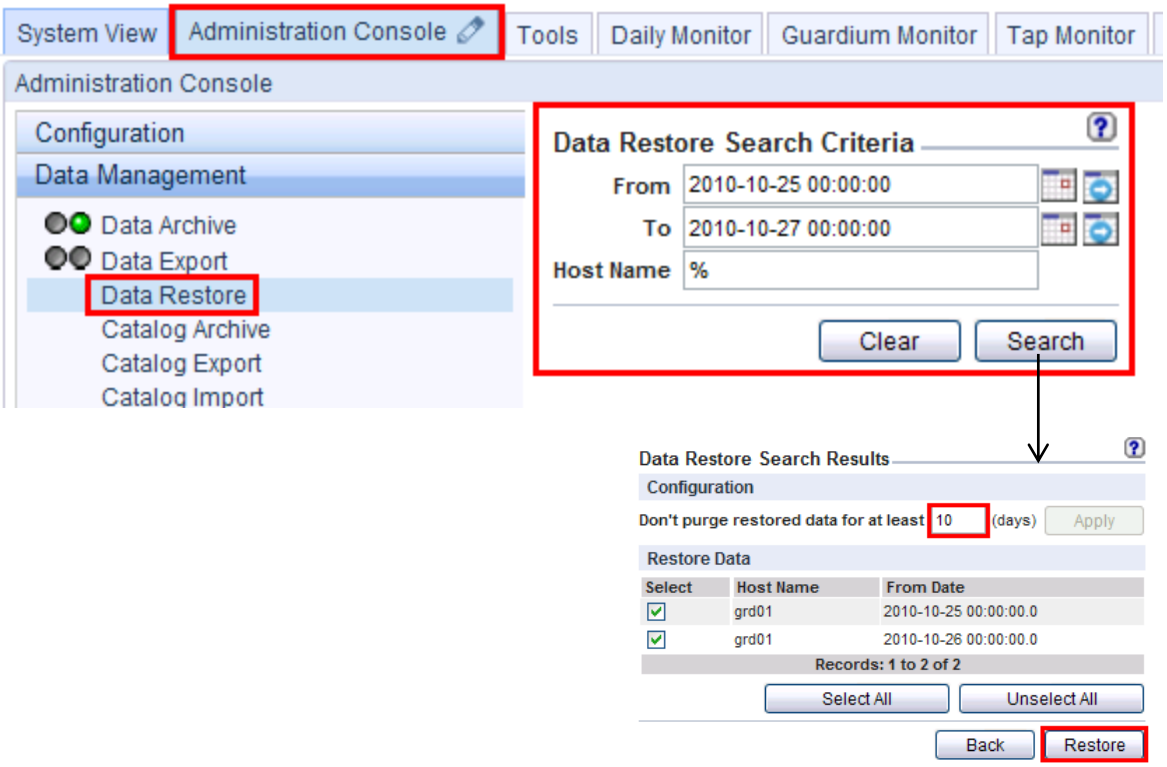
Figure 6-5. Data Management - Data Import (Aggregator only) GU2022.0

Notes:

On the aggregator side, to import data from a collector, you simply need to press **Apply** and **Modify Schedule** to complete the import process.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Data Restore



© Copyright IBM Corporation 2011, 2013

Figure 6-6. Data Management - Data Restore GU2022.0

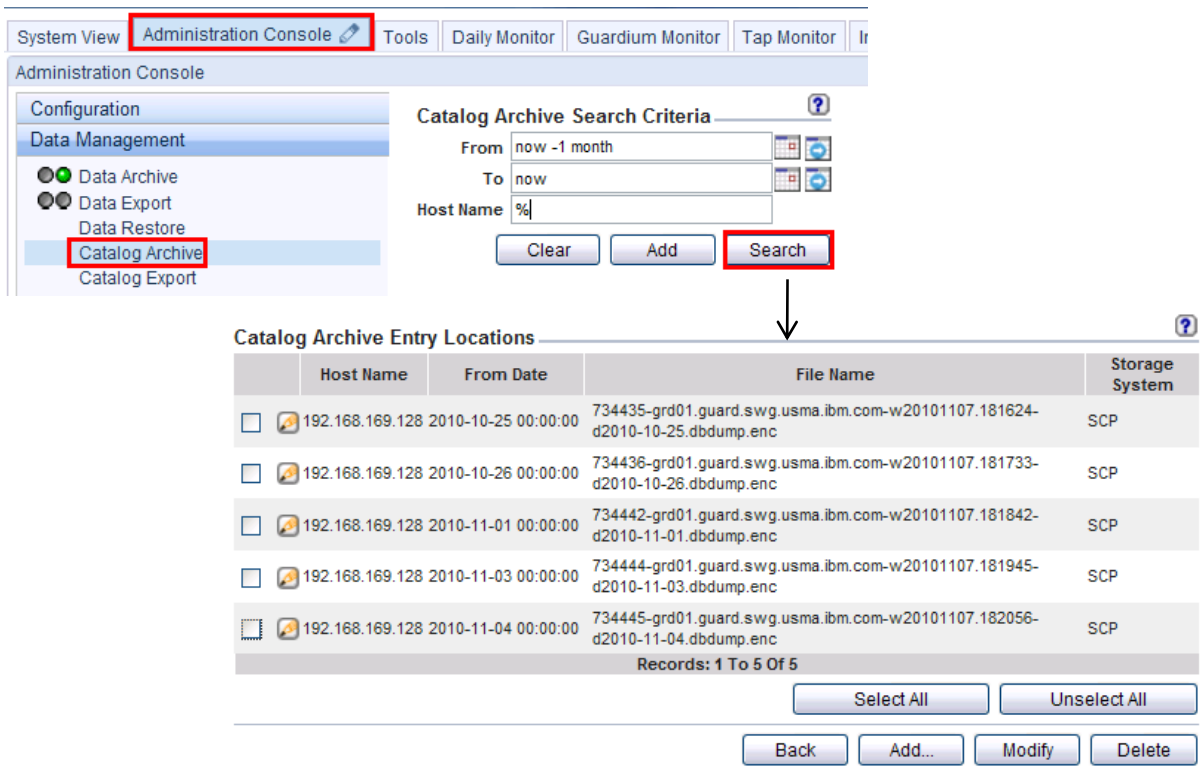
Notes:

Data restore is the opposite of a data archive. To restore data from a an archive file

- Enter a date range and host name (or a % for all hosts) for the archive file that you would like to restore and press **Search**.
- Check the boxes next to the files you would like to restore
- Enter the number of days you would like to retain the newly restored data in the **Don't purge restored data for at least**… field. This will prevent the data from being purged before you have had a chance to review it.
- Press **Restore**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Catalog Archive



© Copyright IBM Corporation 2011, 2013

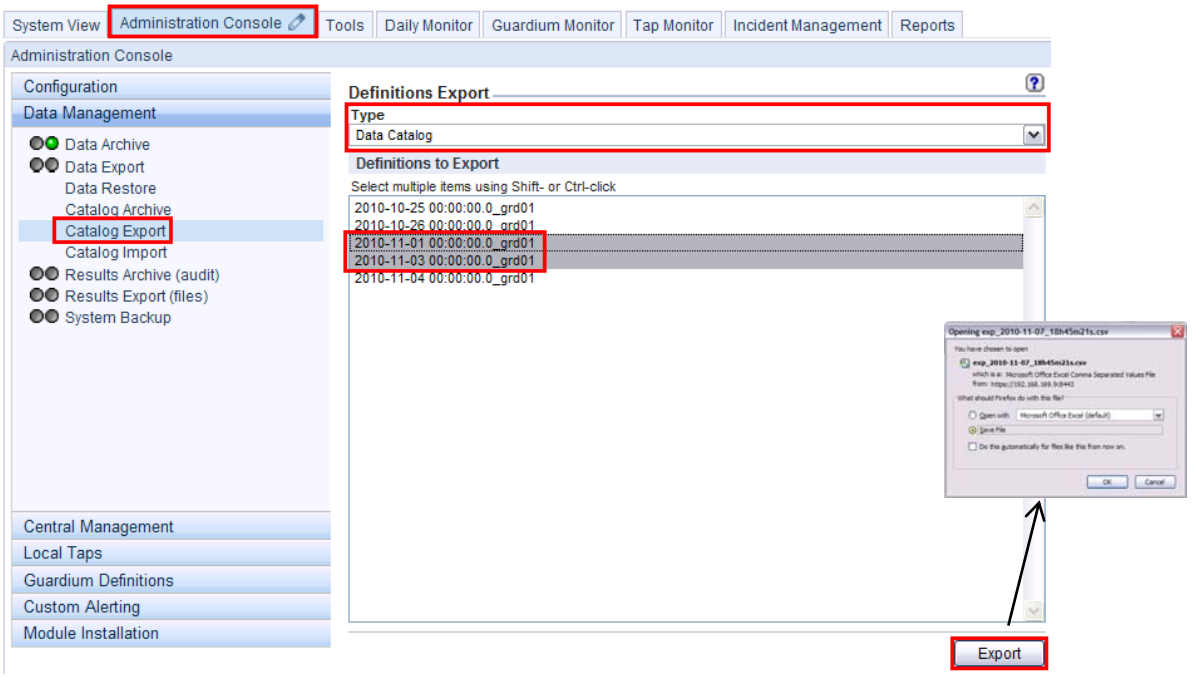
Figure 6-7. Data Management - Catalog Archive GU2022.0

Notes:

Guardium's catalog tracks where every archive file is sent, so that it can be retrieved and restored on the system with minimal effort, at any point in the future. A separate catalog is maintained on each appliance, and a new record is added to the catalog whenever the appliance archives data or results. If archive files are moved to another location after the Guardium archive operation, Guardium has no way of knowing what happened to those files. For these situations, the archive catalog can be maintained manually, using the Catalog Archive command to add or remove archive entries.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Catalog Export



© Copyright IBM Corporation 2011, 2013

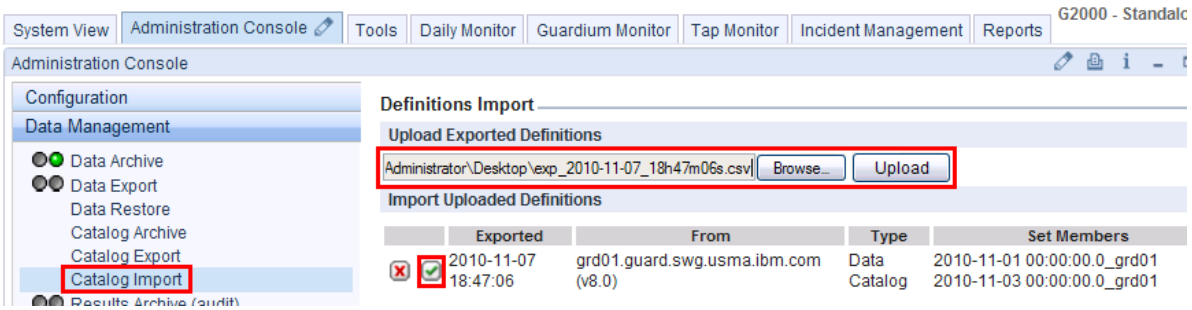
Figure 6-8. Data Management - Catalog Export GU2022.0

Notes:

Catalog export allows you to export either the data or results catalog.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Catalog Import



© Copyright IBM Corporation 2011, 2013

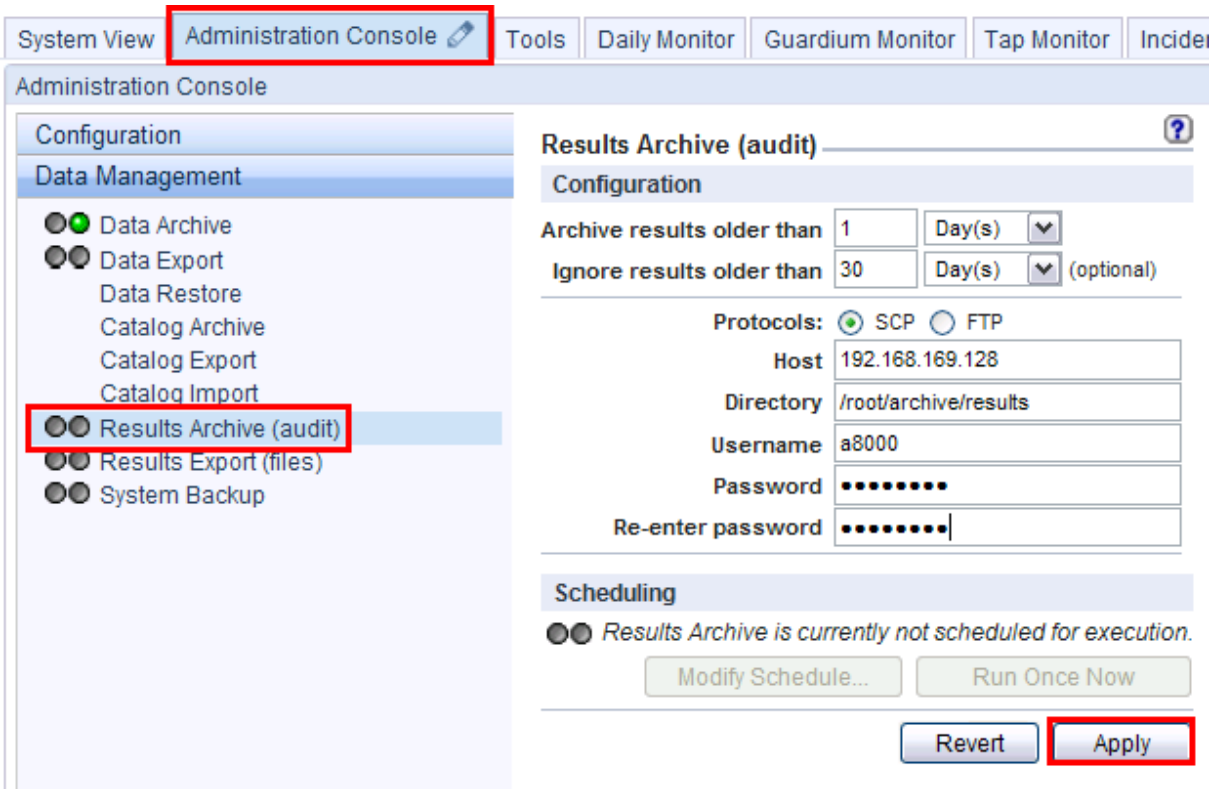
Figure 6-9. Data Management - Catalog Import GU2022.0

Notes:

Catalog import allows you to import a previously exported data or results catalog.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Results Archive (audit)



© Copyright IBM Corporation 2011, 2013

Figure 6-10. Data Management - Results Archive (audit) GU2022.0

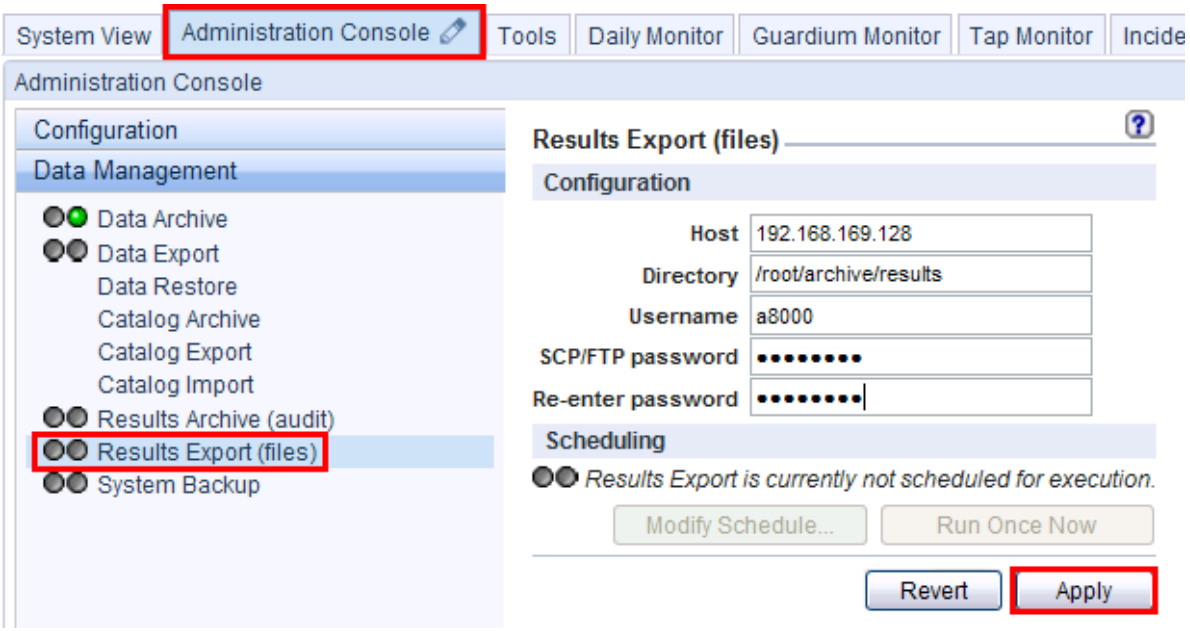
Notes:

Results Archive backs up audit task results (reports, assessment tests, entity audit trail, privacy sets and classification processes) as well as the view and sign-off trails and the accumulated comments from workflow processes. Results sets are purged from the system according to the workflow process definition.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Data Management - Results Export (files)



© Copyright IBM Corporation 2011, 2013

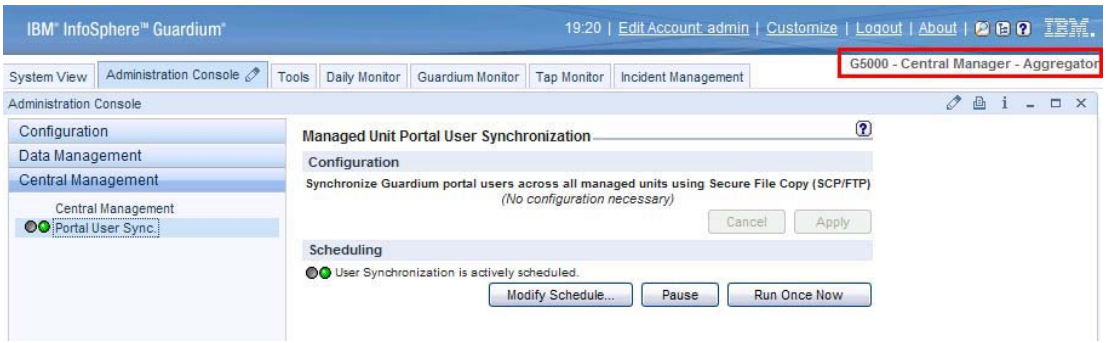
Figure 6-11. Data Management - Results Export (files) GU2022.0

Notes:

CSV, CEF and PDF files can be created by workflow processes. The **Results Export (files)** function exports all such files that are on the appliance.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Administration Console - Central Management



© Copyright IBM Corporation 2011, 2013

Figure 6-12. Administration Console - Central Management GU2022.0

Notes:

In a central management configuration, one Guardium unit is designated as the Central Manager. That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Unmanaged units are referred to as standalone units.

The concept of a "local machine" can refer to any machine in the Central Management system. There are some applications (Audit Processes, Queries, Portlets, etc.) which can be run on both the Managed Units and the Central Manager. In both cases, the definitions come from the Central Manager and the data comes from the local machine (which could also be the Central Manager).

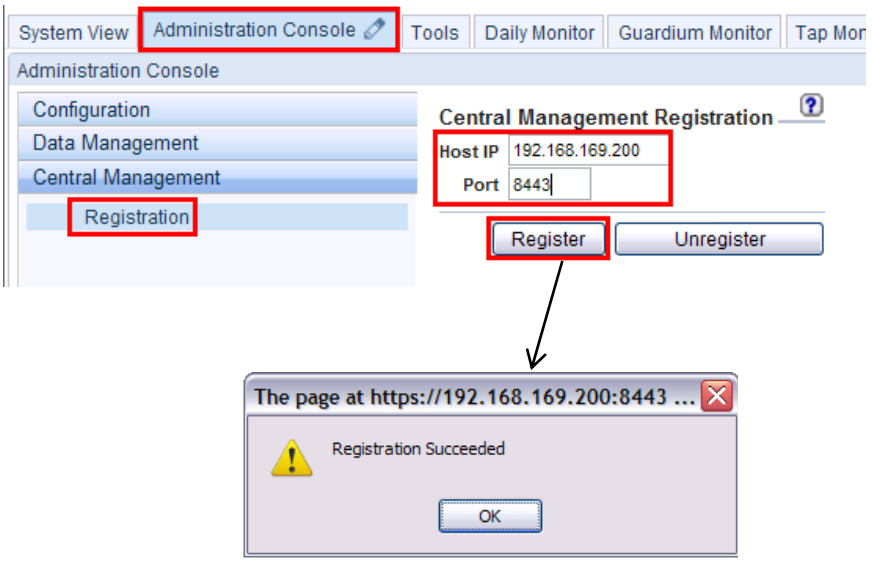
Once a Central Management system is set up, customers can use either the Central Manager or a Managed Unit to create or modify most definitions. Keep in mind that most of the definitions reside on the Central Manager, regardless of which machine the actual editing is done from.

To configure an aggregator as a Central Manager, from the CLI type **store unit type manager**. You will see in the upper right hand corner of the GUI that the system is a Central Manager.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Registering to a CM from a collector



© Copyright IBM Corporation 2011, 2013

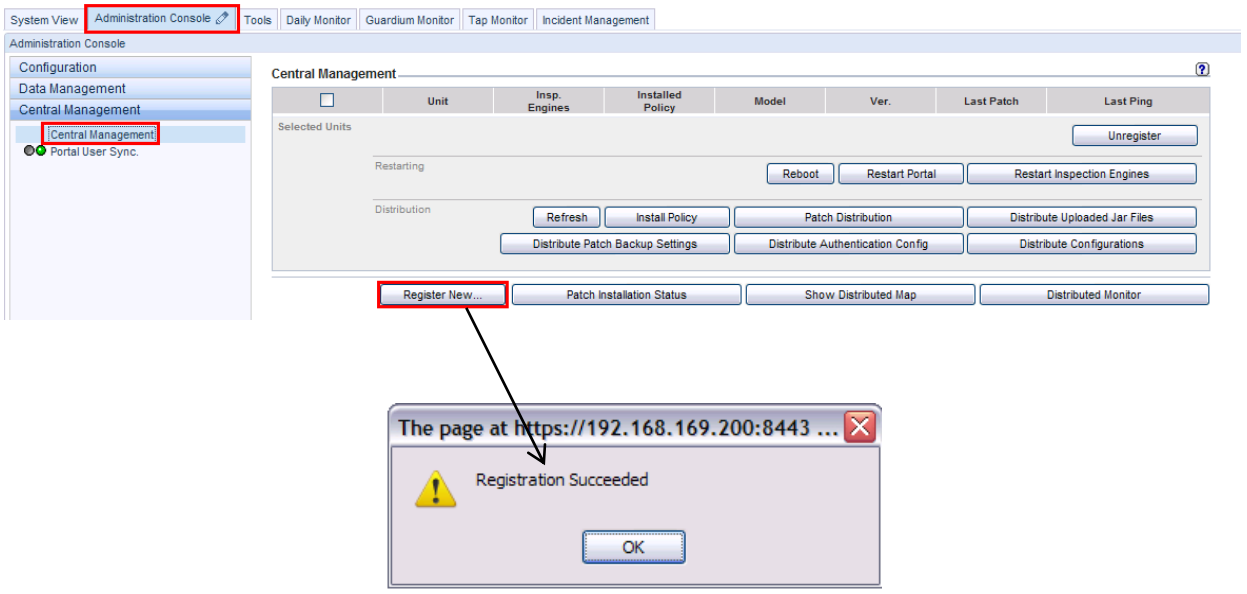
Figure 6-13. Registering to a CM from a collector GU2022.0

Notes:

To register to a Central Manager from a collector, click the **Registration** link. Enter the IP address and port of the Central Manger and press **Register**. The shared secret on the Central Manager and unit to be managed must match to enable registration.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Registering a unit from the Central Manager



© Copyright IBM Corporation 2011, 2013

Figure 6-14. Registering a unit from the Central Manager GU2022.0

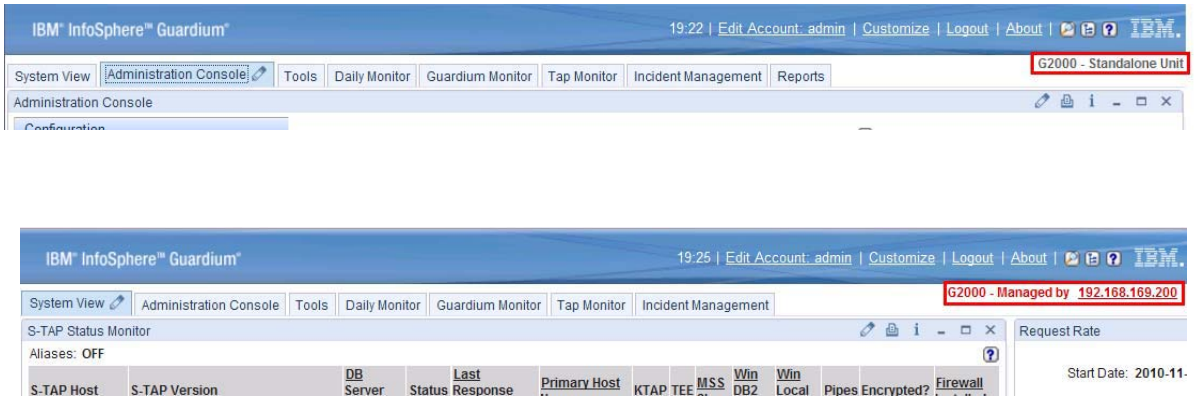
Notes:

You can also register units from the Central Manager. Press the **Central Management** link, press the **Register New** button, enter the IP address of the unit to be managed and press enter.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Standalone versus Managed By



© Copyright IBM Corporation 2011, 2013

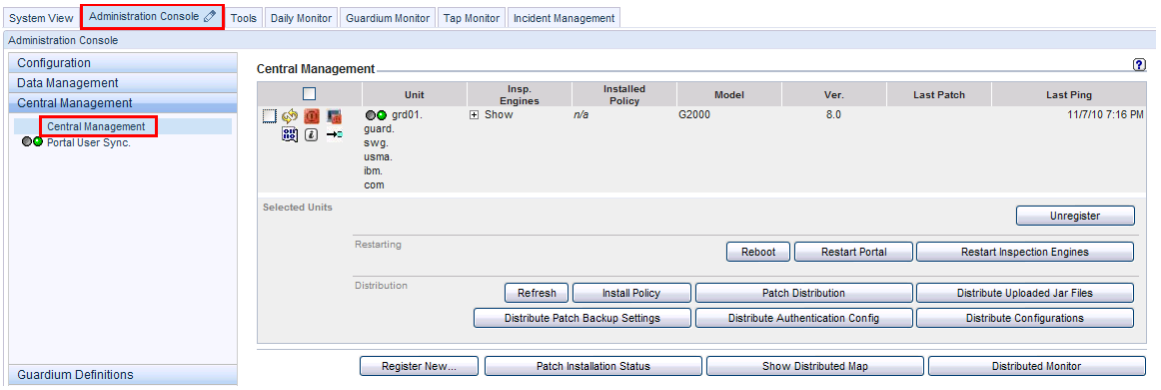
Figure 6-15. Standalone versus Managed By GU2022.0

Notes:

Once a system has been added to a central management environment, the status of the appliance will change from **Standalone Unit** to **Managed by …**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Central Management screen



© Copyright IBM Corporation 2011, 2013

Figure 6-16. Central Management screen GU2022.0

Notes:

From the Central Manager an administrator can

- Register Guardium units for management
- Monitor managed units (unit availability, inspection engine status, etc.)
- View system log files (syslogs) of managed units
- View reports using data on managed units
- View main statistics for managed units
- Install Guardium security policies on managed units
- Restart managed units
- Manage Guardium inspection engines on managed units
- Maintain the complete set of Users, Security Roles, Groups, and Application Role Permissions used on all managed systems
- Distribute patches

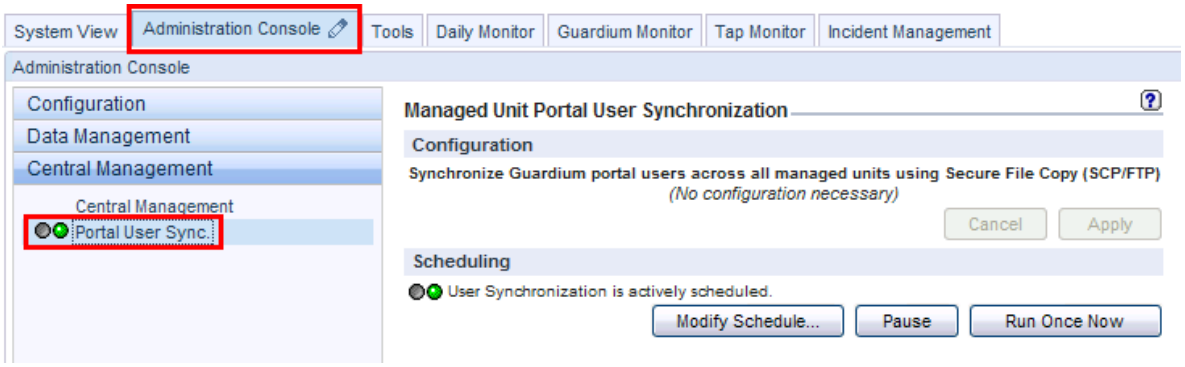
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Distribute Uploaded Jar Files
- Distribute Patch Backup Settings
- Distribute Authentication Config
- Distribute Configurations

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Portal User Sync



© Copyright IBM Corporation 2011, 2013

Figure 6-17. Portal User Sync GU2022.0

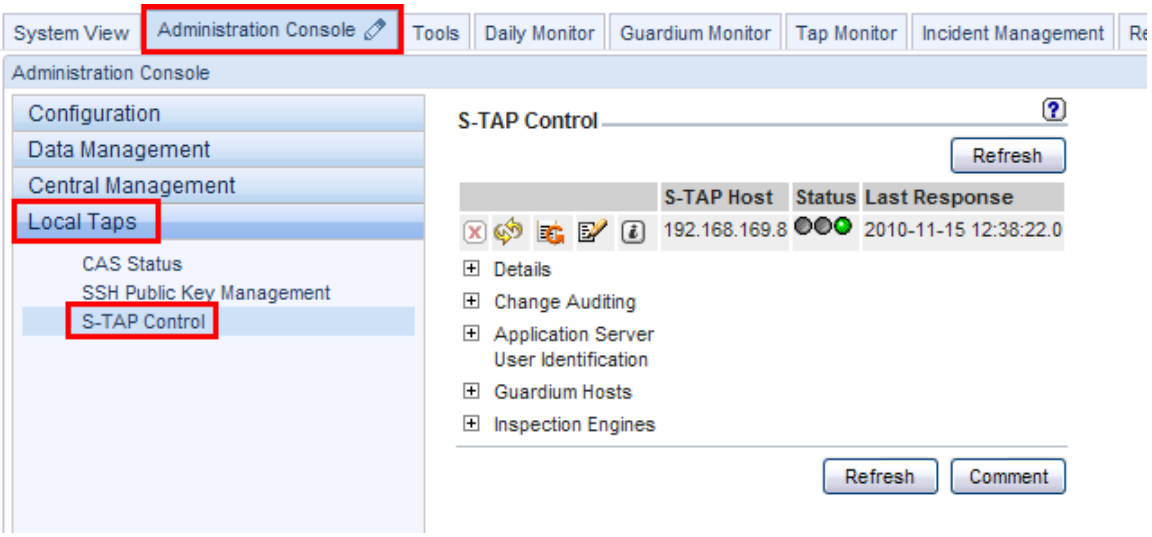
Notes:

The Central Manager controls the definition of Users, Security Roles, and Groups for all managed units. It does this by making an encrypted and signed copy of its complete set of definitions and transmitting that information to all managed units, in addition some other definitions that are required for local processing (Groups and Group members, Audit processes, Aliases and more) are also copied. The managed units then update their internal databases on an hourly basis, which means that there may be a delay of up to an hour between the time users, roles or permissions are added or modified on the Central manager and the time that the managed unit applies those updates.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Local Taps



© Copyright IBM Corporation 2011, 2013

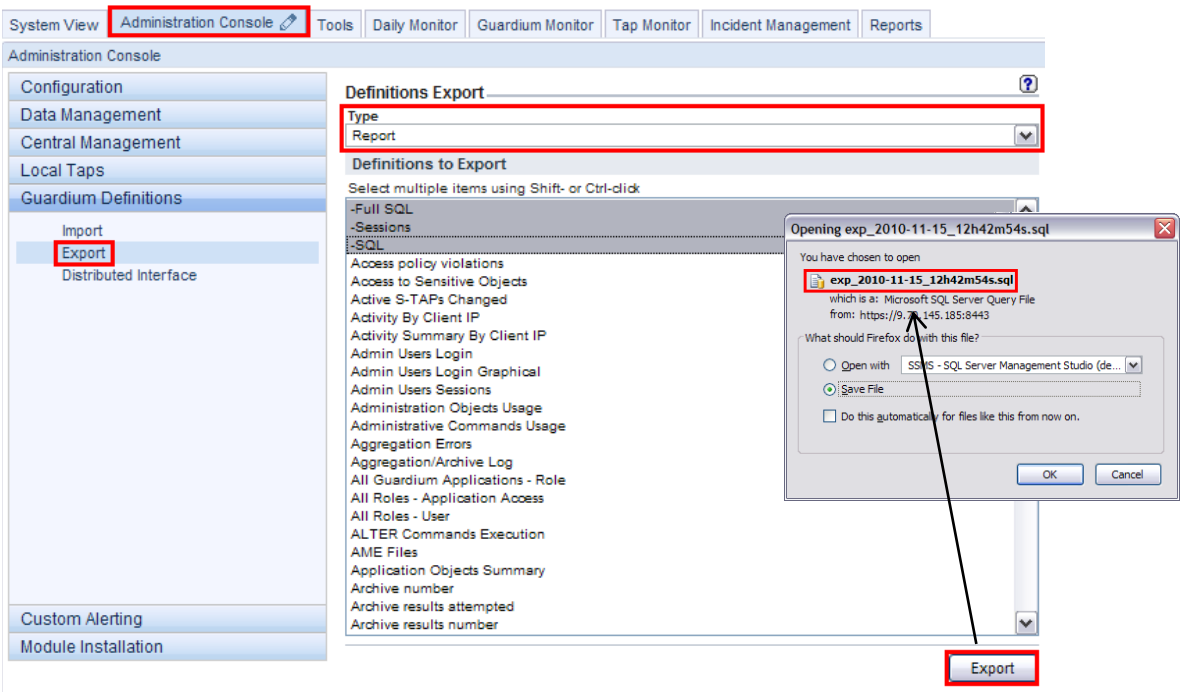
Figure 6-18. Local Taps GU2022.0

Notes:

See the S-TAP and CAS units for detail on configuring Local Taps.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Export definitions



© Copyright IBM Corporation 2011, 2013

Figure 6-19. Export definitions GU2022.0

Notes:

If you have multiple systems with identical or similar requirements, and are not using Central Management, you can define the components you need on one system and export those definitions to other systems, provided those systems are on the same software release level.

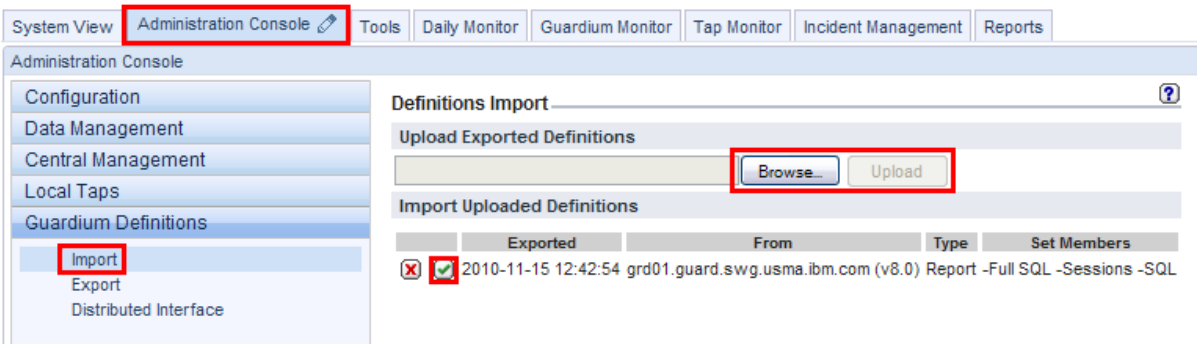
You can export one type of definition (reports, for example) at a time. Each element exported can cause other referenced definitions to be exported as well. For example, a report is always based on a query, and it can also reference other items, such as IP address groups or time periods. All referenced definitions (except for security roles) are exported along with the report definition. However, only one copy of a definition is exported if that definition is referenced in multiple exported items.

An export of policies or queries exports only the groups referenced by the exported policies or queries. Previously an export of policies or queries would export all groups.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Import definitions



© Copyright IBM Corporation 2011, 2013

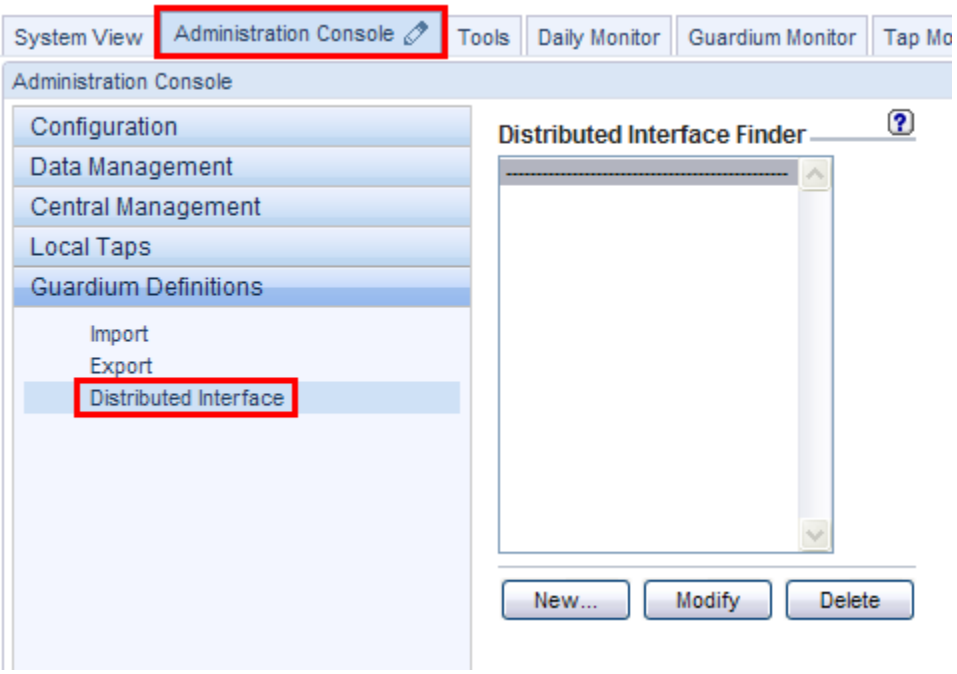
Figure 6-20. Import definitions GU2022.0

Notes:

The **Import** link allows you to import definitions exported from another appliance.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Distributed Interface



© Copyright IBM Corporation 2011, 2013

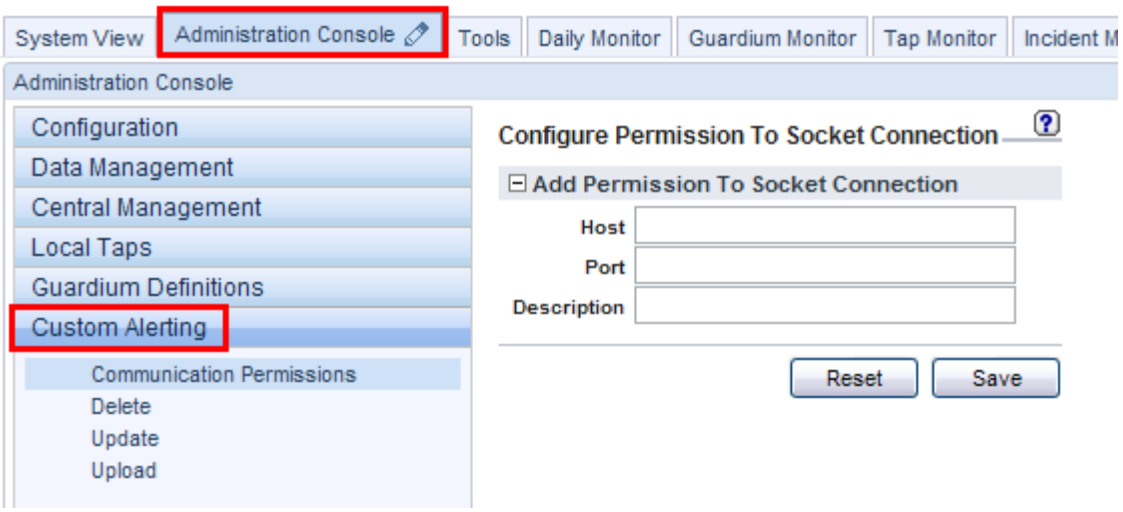
Figure 6-21. Distributed Interface GU2022.0

Notes:

Use this configuration screen to define the Distributed Interface and upload the Protocol Buffer (.proto) file to the DIST_INT database. From this database, Query Domain metadata is built automatically. After the metadata is built, the user can go to Custom Domain Builder to modify or clone the data and build custom reports. The distributed interface data uses protocol buffers. Protocol buffers are a flexible, efficient, and automated mechanism for serializing structured data.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Custom Alerting



© Copyright IBM Corporation 2011, 2013

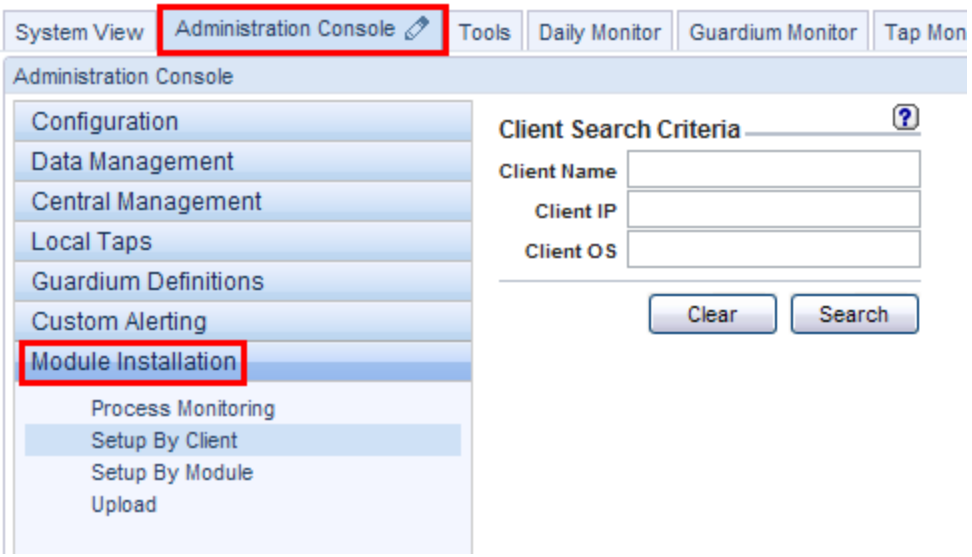
Figure 6-22. Custom Alerting GU2022.0

Notes:

Custom alerting allows users to upload custom Java classed to be used in policy and correlation alerts.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Module Installation



© Copyright IBM Corporation 2011, 2013

Figure 6-23. Module Installation GU2022.0

Notes:

Module installation allows you to apply modules to Guardium agents. See the GIM/STAP unit for further details.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. A data _____ backs up the data that has been captured by an appliance during a given time period.

2. A data _____ deletes the data that has been captured by an appliance during a given time period.

3. A data _____ sends the data that has been captured by an appliance during a given time period to an aggregator.

4. The Guardium _____ tracks every archive file and where it is stored, so that the file can be easily retrieved and restored.

5. True or false: Only an aggregator can perform a data import operation

6. Once a system has been added to a central management environment, the status of the appliance will change from _____ to _____.

© Copyright IBM Corporation 2011, 2013

Figure 6-24. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. A data **archive** backs up the data that has been captured by an appliance during a given time period.
2. A data **purge** deletes the data that has been captured by an appliance during a given time period.
3. A data **export** sends the data that has been captured by an appliance during a given time period to an aggregator.
4. The Guardium **catalog** tracks every archive file and where it is stored, so that the file can be easily retrieved and restored.
5. **True** or false: Only an aggregator can perform a data import operation
6. Once a system has been added to a central management environment, the status of the appliance will change from **standalone** (unit) to **mangaged by.**

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (2 of 2)

7. True or false: The current day's data cannot be archived.

8. The opposite of an archive is a(n) _____.

9. The maximum number of Central Managers in a Guardium environment is _____.

10. There could be a time lag of up to one _____ between the time users, roles, or permissions are added to the Central Manager and the time they are applied to the managed units.

© Copyright IBM Corporation 2011, 2013

Figure 6-25. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

7.

8.

9.

10.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

7. **True** or false: The current day's data cannot be archived.
8. The opposite of an archive is a **restore**.
9. The maximum number of Central Managers in a Guardium environment is **one**.
10. There could be a time lag of up to one **hour** between the time users, roles, or permissions are added to the Central Manager and the time they are applied to the managed units.

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Configure an IBM InfoSphere Guardium appliance from the Administration Console

© Copyright IBM Corporation 2011, 2013

Figure 6-26. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 3** in the Exercise Guide.

© Copyright IBM Corporation 2011, 2013

Figure 6-27. Exercise GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (1 of 2)

1. A data **archive** backs up the data that has been captured by an appliance during a given time period.

2. A data **purge** deletes the data that has been captured by an appliance during a given time period.

3. A data **export** sends the data that has been captured by an appliance during a given time period to an aggregator.

4. The Guardium **catalog** tracks every archive file and where it is stored, so that the file can be easily retrieved and restored.

5. **True** or false: Only an aggregator can perform a data import operation

6. Once a system has been added to a central management environment, the status of the appliance will change from **standalone** (unit) to **mangaged by.**

© Copyright IBM Corporation 2011, 2013

Figure 6-28. Checkpoint solution (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (2 of 2)

7. **True** or false: The current day's data cannot be archived.

8. The opposite of an archive is a(n) **restore**.

9. The maximum number of Central Managers in a Guardium environment is **one**.

10. There could be a time lag of up to one **hour** between the time users, roles, or permissions are added to the Central Manager and the time they are applied to the managed units.

© Copyright IBM Corporation 2011, 2013

Figure 6-29. Checkpoint solution (2 of 2) GU2022.0

Notes:

Write your answers here:

7.

8.

9.

10.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 7. S-TAP and GIM

Estimated time

01:30

What this unit is about

This unit describes S-TAP and how to install it on either a Windows or a Linux system.

What you should be able to do

After completing this unit, you should be able to:

- Understand S-TAP
- Install S-TAP on Windows interactively
- Install S-TAP on Linux using GIM
- Understand the non-interactive installation methods

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand S-TAP
- Install S-TAP on Windows interactively
- Install S-TAP on Linux using GIM
- Understand the non-interactive installation methods

© Copyright IBM Corporation 2011, 2013

Figure 7-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP overview

- S-TAP
- Lightweight agent installed on the database server
- Monitors:
  - Local traffic
  - Network traffic
- Handles encrypted logins
- Supports:
  - Windows
  - UNIX

© Copyright IBM Corporation 2011, 2013

Figure 7-2. S-TAP overview GU2022.0

Notes:

Guardium's S-TAP is an optional, lightweight software agent installed on a database server system. It monitors database traffic and forwards information about that traffic to a Guardium appliance.

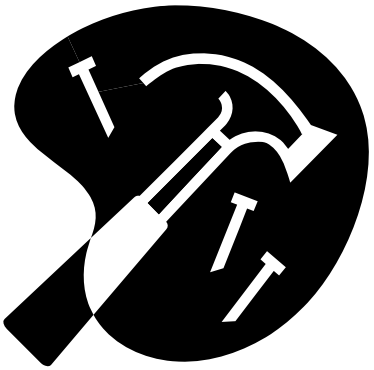
S-TAP can monitor database traffic that is local to that system. This is important because local connections can provide "back door" access to the database - and all such access needs to be monitored and audited.

S-TAP can be used to monitor any network traffic that is visible from the database server on which it is installed. S-TAP can also handle encrypted logins more effictively than traffic originating from a Span port or network tap.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP installation methods

- Three ways to install S-Tap:
  1. Interactive S-TAP Installer
  2. Guardium Installation Manager (GIM)
  3. Silent, non-interactive installation using GuardAPI



© Copyright IBM Corporation 2011, 2013

Figure 7-3. S-TAP installation methods GU2022.0

Notes:

S-TAP can be installed remotely from the command line on both Windows or Unix servers. It can also be installed through the Guardium Installation Manager. For enterprise deployments, the S-TAP installation can be scripted and installed non-interactively.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP ports

- 8081 (TCP)
  - GIM to Appliance traffic for both UNIX and Windows
- 16016 (TCP)
  - Unencrypted STAP Unix traffic
- 16017 (TLS)
  - Encrypted STAP Unix traffic
- 9500 (TCP)
  - Unencrypted STAP Windows traffic
- 9501 (TCP)
  - Encrypted STAP Windows traffic
- 8075 (UDP)
  - STAP heartbeat (Windows only)

© Copyright IBM Corporation 2011, 2013

Figure 7-4. S-TAP ports GU2022.0

Notes:

If the database server and collector are on opposite sides of a firewall, you must make sure that the appropriate ports are open for the components to communicate correctly. A closed firewall port is the most common configuration error when deploying S-TAP.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Installation resources

Resource materials include:

- *s_tap_help_book.pdf*
- *Guardium_Installation_Manager.pdf*
- *IBM InfoSphere Guardium 8 STAP Installation and Configuration yyyy-mm-dd*.doc

© Copyright IBM Corporation 2011, 2013

Figure 7-5. Installation resources GU2022.0

Notes:

When installing S-TAP, these documents will help ensure that you have all covered all the installation prerequisites and have completed all of the required steps.

- *s_tap_help_book.pdf* – available from the on-line help
- *Guardium_Installation_Manager.pdf* - available from the on-line help
- *IBM InfoSphere Guardium 9 STAP Installation and Configuration yyyy-mm-dd.doc* – provided by your professional services consultant Guardium technical support

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

7.1. Interactive installation: Windows

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Interactive installation: Windows

After completing this topic, you should be able to:

- Use the interactive installation method to setup S-TAP on a Windows database server
- Manually configure a Microsoft SQL Server inspection engine
- Verify the installation of an inspection engine

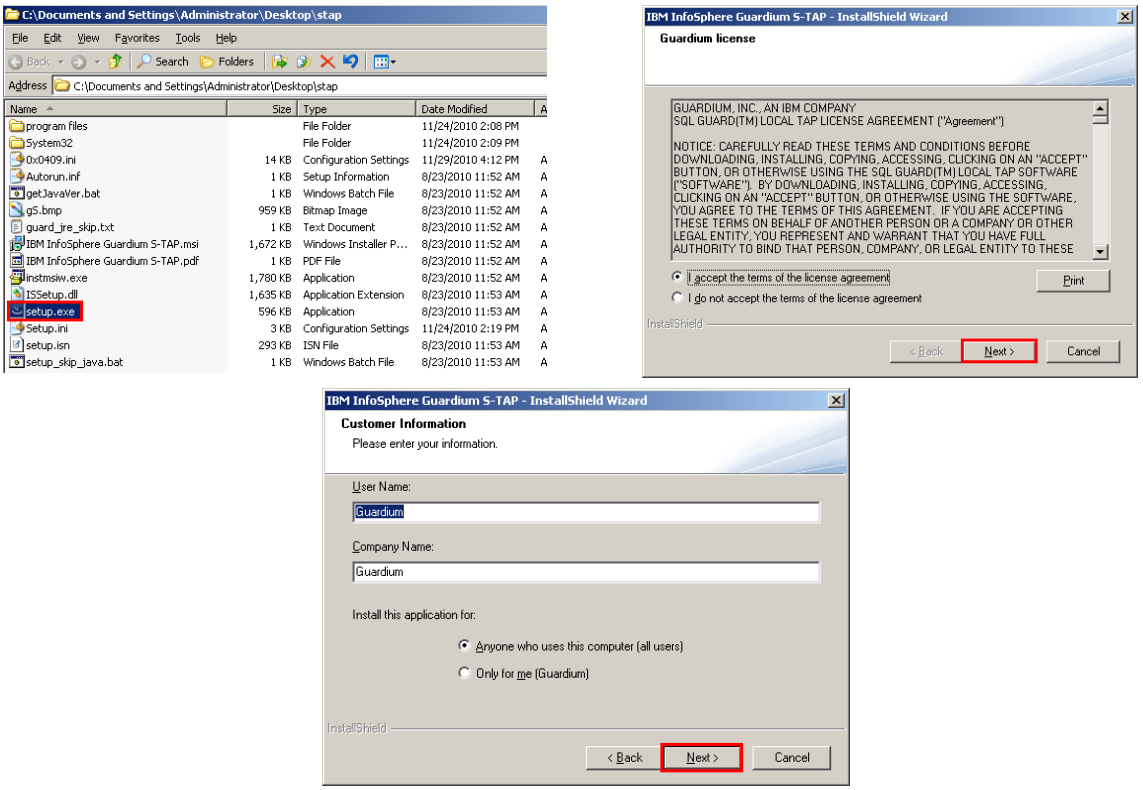
© Copyright IBM Corporation 2011, 2013

Figure 7-6. Interactive installation: Windows GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Windows STAP interactive installation: setup.exe


C:\Documents and Settings\Administrator\Desktop\stap
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\stap
Name Size Type Date Modified
program files File Folder 11/24/2010 2:08 PM
System32 File Folder 11/24/2010 2:09 PM
0x0409.ini 14 KB Configuration Settings 11/29/2010 4:12 PM
Autorun.inf 1 KB Setup Information 8/23/2010 11:52 AM
getJavaVer.bat 1 KB Windows Batch File 8/23/2010 11:52 AM
g5.bmp 959 KB Bitmap Image 8/23/2010 11:52 AM
guard_jre_skip.txt 1 KB Text Document 8/23/2010 11:52 AM
IBM InfoSphere Guardium S-TAP.msi 1,672 KB Windows Installer P... 8/23/2010 11:52 AM
IBM InfoSphere Guardium S-TAP.pdf 1 KB PDF File 8/23/2010 11:52 AM
instmsiw.exe 1,780 KB Application 8/23/2010 11:52 AM
ISSetup.dll 1,635 KB Application Extension 8/23/2010 11:53 AM
setup.exe 596 KB Application 8/23/2010 11:53 AM
Setup.ini 3 KB Configuration Settings 11/24/2010 2:19 PM
setup.isn 293 KB ISN File 8/23/2010 11:53 AM
setup_skip_java.bat 1 KB Windows Batch File 8/23/2010 11:53 AM
IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Guardium license
GUARDIUM, INC., AN IBM COMPANY
SQL GUARD(TM) LOCAL TAP LICENSE AGREEMENT ("Agreement")
NOTICE: CAREFULLY READ THESE TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE SQL GUARD(TM) LOCAL TAP SOFTWARE ("SOFTWARE"). BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back Next > Cancel
IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Customer Information
Please enter your information.
User Name:
Guardium
Company Name:
Guardium
Install this application for:
Anyone who uses this computer (all users)
Only for me (Guardium)
InstallShield
< Back Next > Cancel

© Copyright IBM Corporation 2011, 2013

Figure 7-7. Windows STAP interactive installation: setup.exe GU2022.0

Notes:

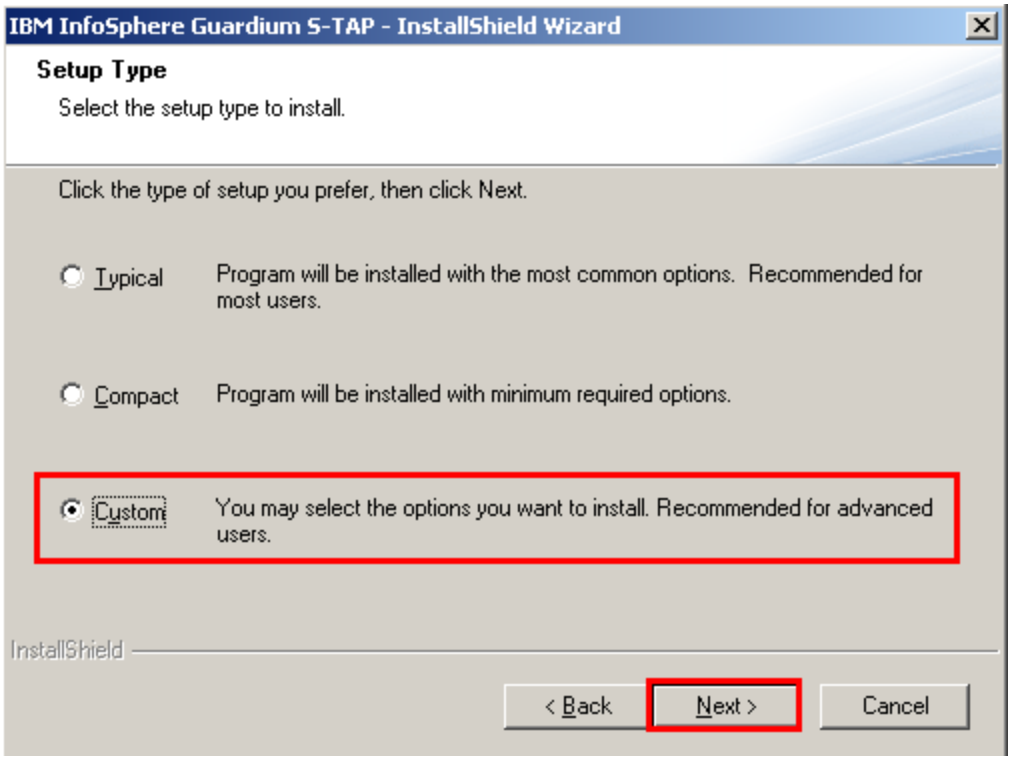
This section will demonstrate how to install S-TAP using the standard Windows' installer (InstallShield). Windows S-TAP can also be installed using the Guardium Installation Manager (GIM) or from the command line using a non-interactive installer.

Follow these steps to install S-TAP on Windows:

- Download the Windows S-TAP installer from IBM
- Run **setup.exe**
- Accept the license and press **Next**
- Enter your *User Name* and *Company Name*
- Press **Next**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Setup type: Custom


IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Setup Type
Select the setup type to install.
Click the type of setup you prefer, then click Next.
Typical
Program will be installed with the most common options. Recommended for most users.
Compact
Program will be installed with minimum required options.
Custom
You may select the options you want to install. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

© Copyright IBM Corporation 2011, 2013

Figure 7-8. Setup type: Custom GU2022.0

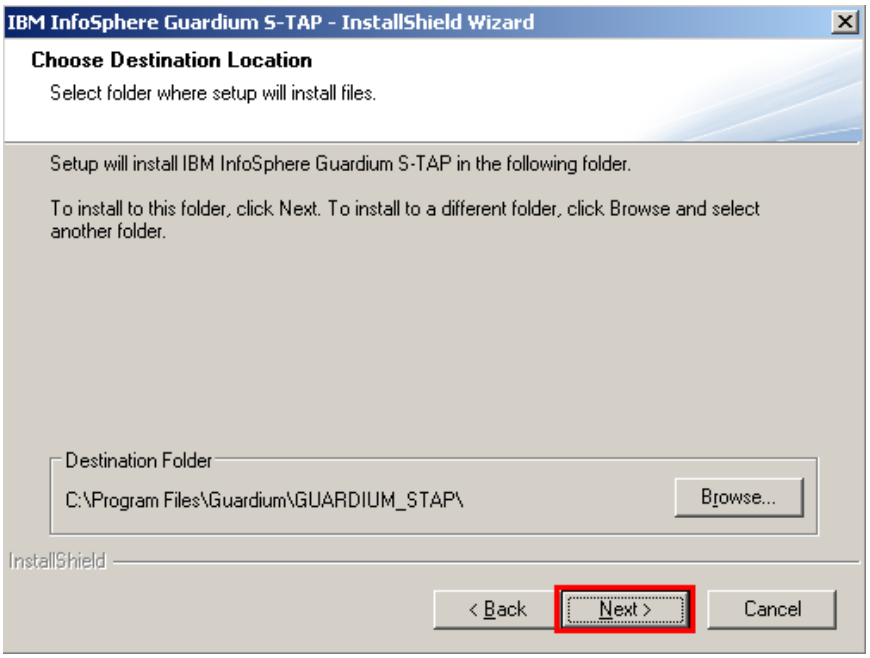
Notes:

Under *Select Type*, choose **Custom** and press **Next**. Always choose a custom installation to avoid installing unnecessary drivers.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Choose Destination Location


IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Choose Destination Location
Select folder where setup will install files.
Setup will install IBM InfoSphere Guardium S-TAP in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\Guardium\GUARDIUM_STAP\
Browse...
InstallShield
< Back
Next >
Cancel

© Copyright IBM Corporation 2011, 2013

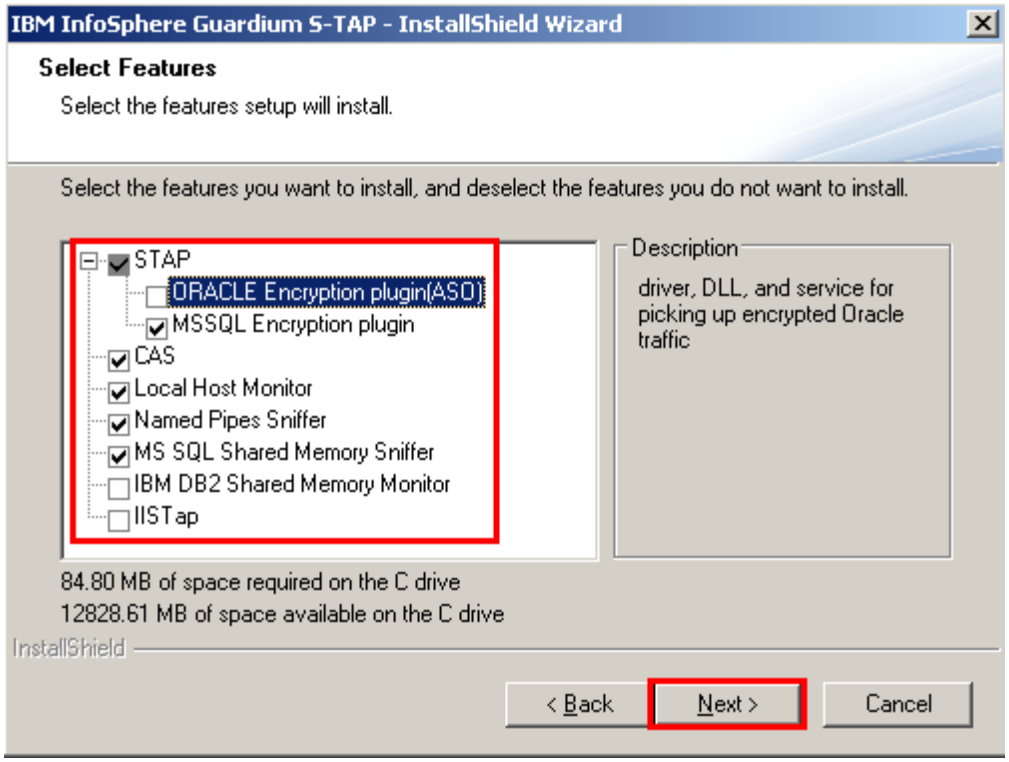
Figure 7-9. Choose Destination Location GU2022.0

Notes:

On the *Choose Destination Location* screen press **Next** to install in the default location or press 'Browse' to select an alternate location.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Select Features


IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Select Features
Select the features setup will install.
Select the features you want to install, and deselect the features you do not want to install.
STAP
ORACLE Encryption plugin(ASO)
MSSQL Encryption plugin
CAS
Local Host Monitor
Named Pipes Sniffer
MS SQL Shared Memory Sniffer
IBM DB2 Shared Memory Monitor
IISTap
Description
driver, DLL, and service for picking up encrypted Oracle traffic
84.80 MB of space required on the C drive
12828.61 MB of space available on the C drive
InstallShield
< Back
Next >
Cancel

© Copyright IBM Corporation 2011, 2013

Figure 7-10. Select Features GU2022.0

Notes:

Confirm that the options that you would like to install are checked, and uncheck those that are not needed. If a specific database type is not hosted on the database server, be sure to uncheck those boxes so that the drivers are not installed.

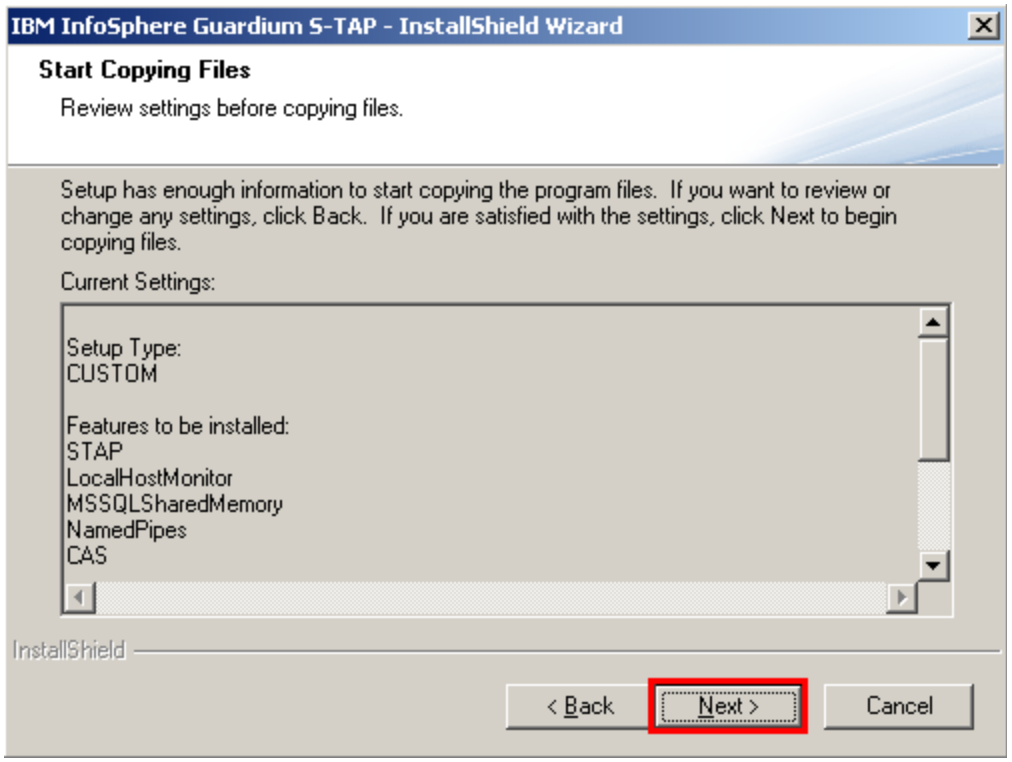
In this example, we are installing S-TAP on a Microsoft SQL Server, so the options to pick are:

- MSSQL encryption plugin
- CAS (optional)
- Local Host Monitor
- Named Pipes Sniffer
- MS SQL Shared Memory Sniffer

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Copy Files


IBM InfoSphere Guardium S-TAP - InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Setup Type:
CUSTOM
Features to be installed:
STAP
LocalHostMonitor
MSSQLSharedMemory
NamedPipes
CAS
InstallShield
< Back
Next >
Cancel

© Copyright IBM Corporation 2011, 2013

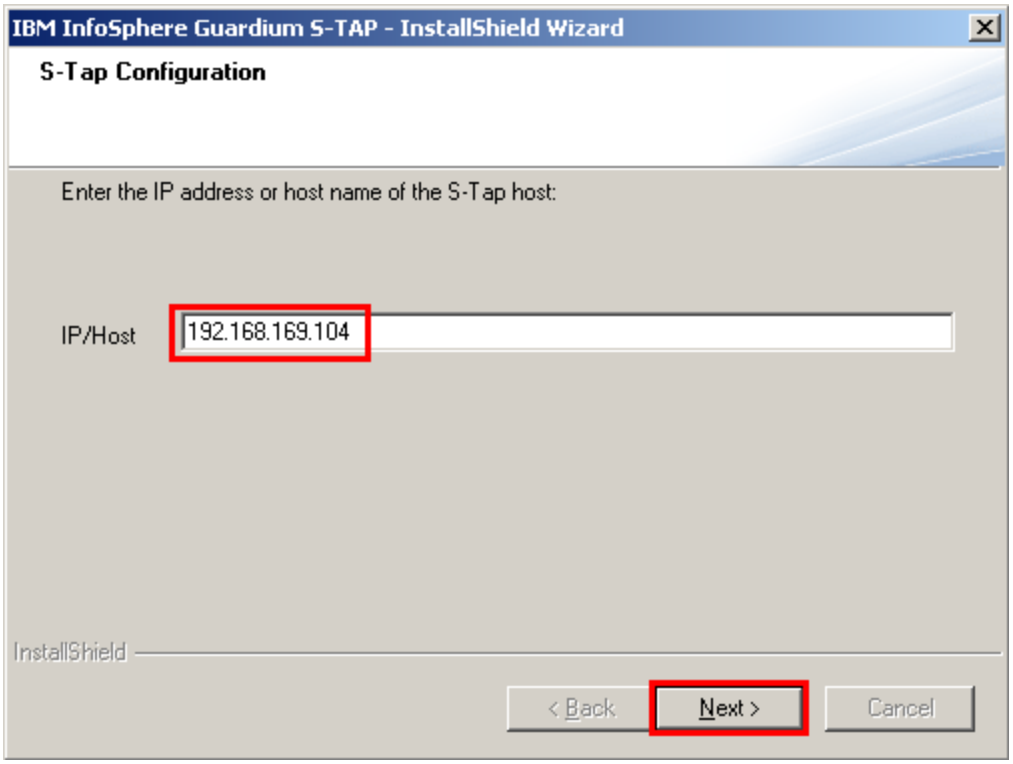
Figure 7-11. Copy Files GU2022.0

Notes:

Confirm that the *Current Settings* are correct and press **Next**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP host



© Copyright IBM Corporation 2011, 2013

Figure 7-12. S-TAP host GU2022.0

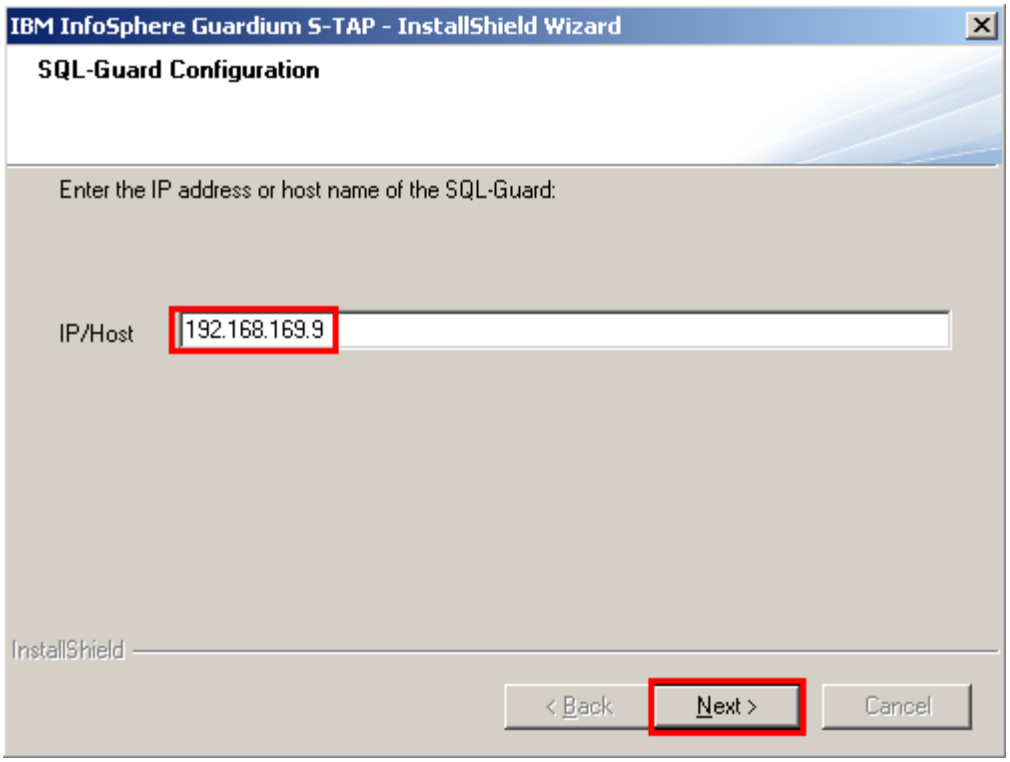
Notes:

For the *IP address or host name of the S-Tap host* enter the **IP Address** or **Fully Qualified Domain** of the **database server** on which you are installing S-TAP in the *IP/Host* field.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Collector IP address



© Copyright IBM Corporation 2011, 2013

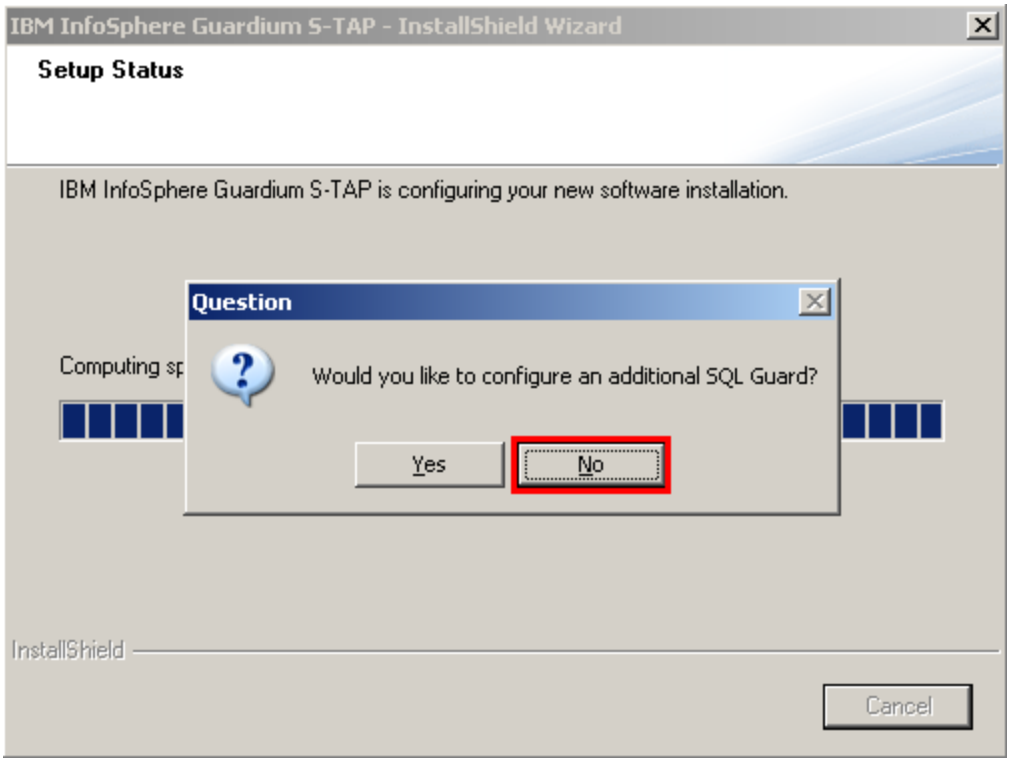
Figure 7-13. Collector IP address GU2022.0

Notes:

For the *IP address or host name of the SQL-Guard* enter the **IP Address** or **Fully Qualified Domain** of the **collector** to which you would like to forward database traffic.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Additional collector for failover



© Copyright IBM Corporation 2011, 2013

Figure 7-14. Additional collector for failover GU2022.0

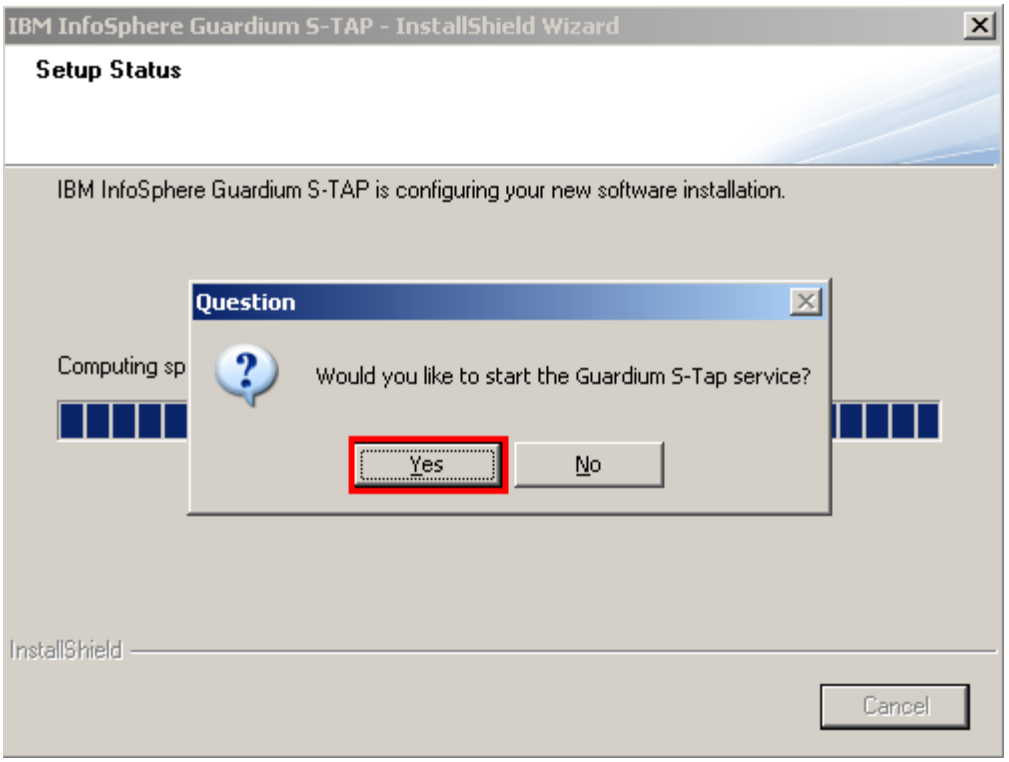
Notes:

If you would like to configure a secondary collector for failover or load balancing press the 'Yes' button. This can be completed from the Guardium GUI also. In most cases, you would press **No** here.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Start S-TAP service



© Copyright IBM Corporation 2011, 2013

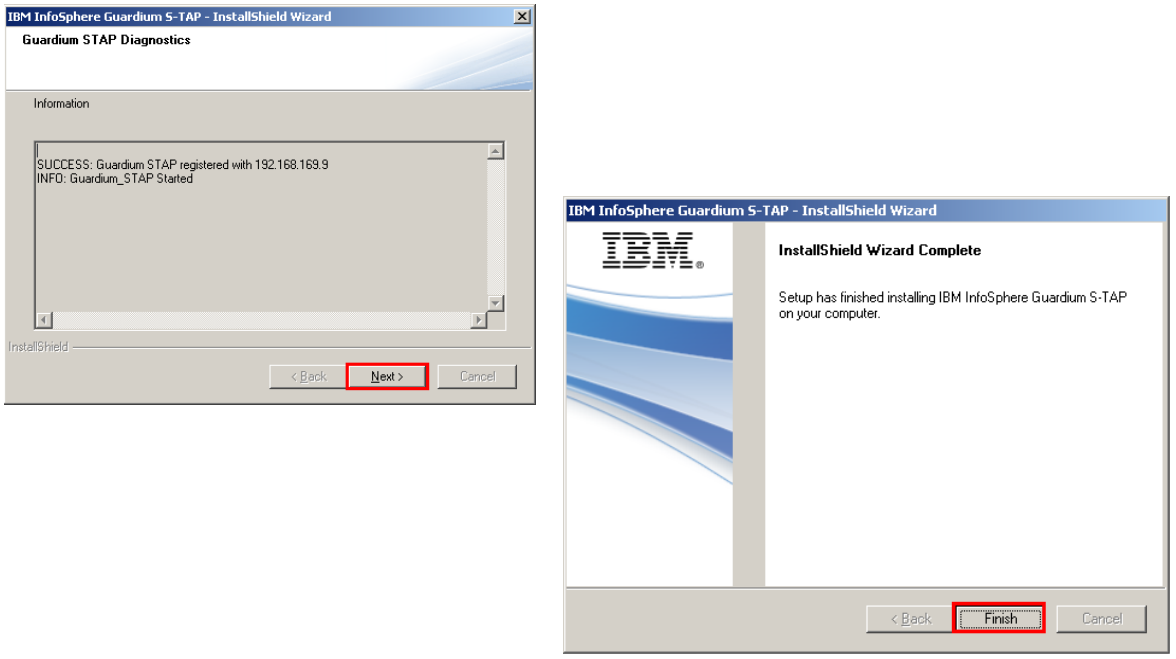
Figure 7-15. Start S-TAP service GU2022.0

Notes:

Press **Yes** to start the S-TAP services.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Complete installation



© Copyright IBM Corporation 2011, 2013

Figure 7-16. Complete installation GU2022.0

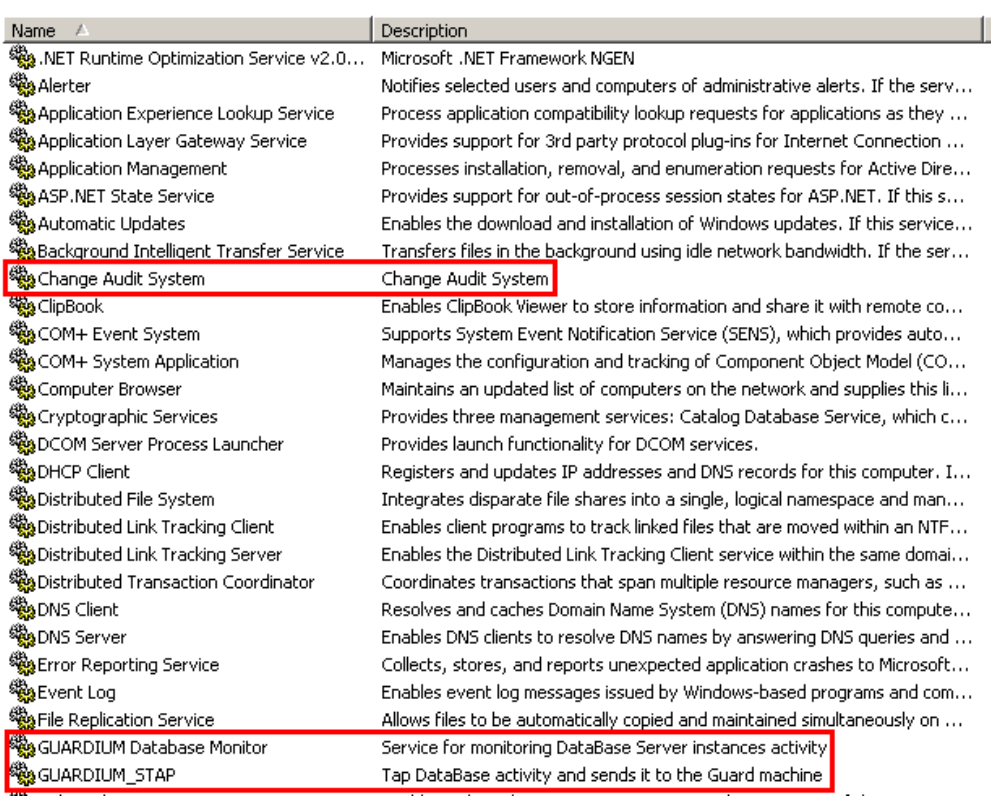
Notes:

The next page will inform you if S-TAP started successfully or not. Confirm that it the services have started and press **Next**. Finally, press **Finish** to complete the installation.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Confirm services


Name
Description
.NET Runtime Optimization Service v2.0...
Microsoft .NET Framework NGEN
Alerter
Notifies selected users and computers of administrative alerts. If the serv...
Application Experience Lookup Service
Process application compatibility lookup requests for applications as they ...
Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection ...
Application Management
Processes installation, removal, and enumeration requests for Active Dire...
ASP.NET State Service
Provides support for out-of-process session states for ASP.NET. If this s...
Automatic Updates
Enables the download and installation of Windows updates. If this service...
Background Intelligent Transfer Service
Transfers files in the background using idle network bandwidth. If the ser...
Change Audit System
Change Audit System
ClipBook
Enables ClipBook Viewer to store information and share it with remote co...
COM+ Event System
Supports System Event Notification Service (SENS), which provides auto...
COM+ System Application
Manages the configuration and tracking of Component Object Model (CO...
Computer Browser
Maintains an updated list of computers on the network and supplies this li...
Cryptographic Services
Provides three management services: Catalog Database Service, which c...
DCOM Server Process Launcher
Provides launch functionality for DCOM services.
DHCP Client
Registers and updates IP addresses and DNS records for this computer. I...
Distributed File System
Integrates disparate file shares into a single, logical namespace and man...
Distributed Link Tracking Client
Enables client programs to track linked files that are moved within an NTF...
Distributed Link Tracking Server
Enables the Distributed Link Tracking Client service within the same domai...
Distributed Transaction Coordinator
Coordinates transactions that span multiple resource managers, such as ...
DNS Client
Resolves and caches Domain Name System (DNS) names for this compute...
DNS Server
Enables DNS clients to resolve DNS names by answering DNS queries and ...
Error Reporting Service
Collects, stores, and reports unexpected application crashes to Microsoft...
Event Log
Enables event log messages issued by Windows-based programs and com...
File Replication Service
Allows files to be automatically copied and maintained simultaneously on ...
GUARDIUM Database Monitor
Service for monitoring DataBase Server instances activity
GUARDIUM_STAP
Tap DataBase activity and sends it to the Guard machine

© Copyright IBM Corporation 2011, 2013

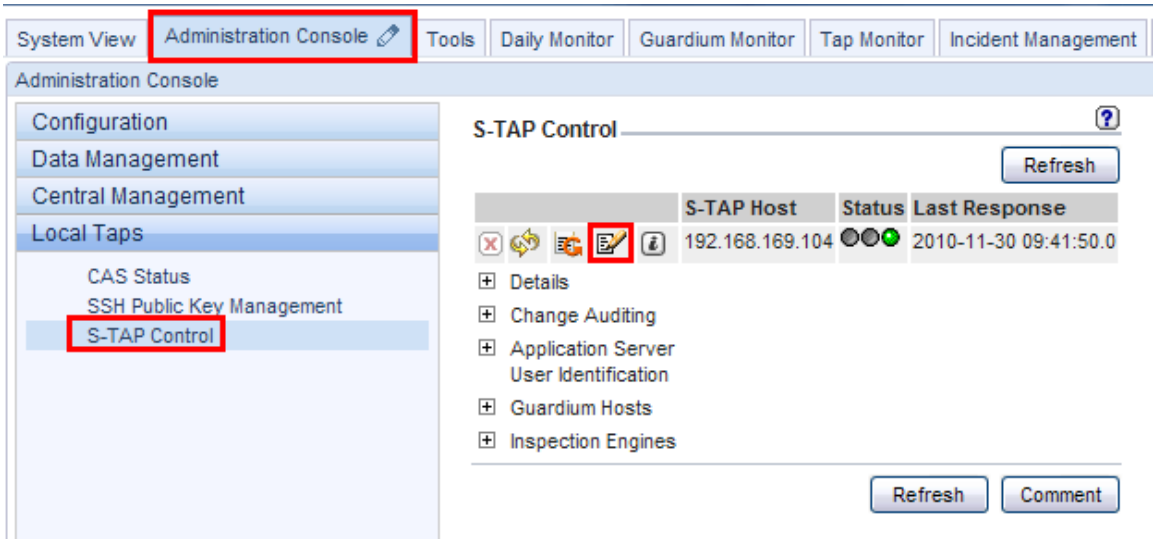
Figure 7-17. Confirm services GU2022.0

Notes:

After completing the installation confirm that the **GUARDIUM_STAP** and the **GUARDIUM Database Monitor** services are running. Also, if you installed CAS, confirm that the **Change Audit System** is running.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP Control status



© Copyright IBM Corporation 2011, 2013

Figure 7-18. S-TAP Control status GU2022.0

Notes:

Next, log into the Guardium Console as admin (or a user in the admin role). Go to **Administration Console** > **Local Taps** > **S-TAP Control**. You should see the newly installed S-TAP with a green light under *Status*.

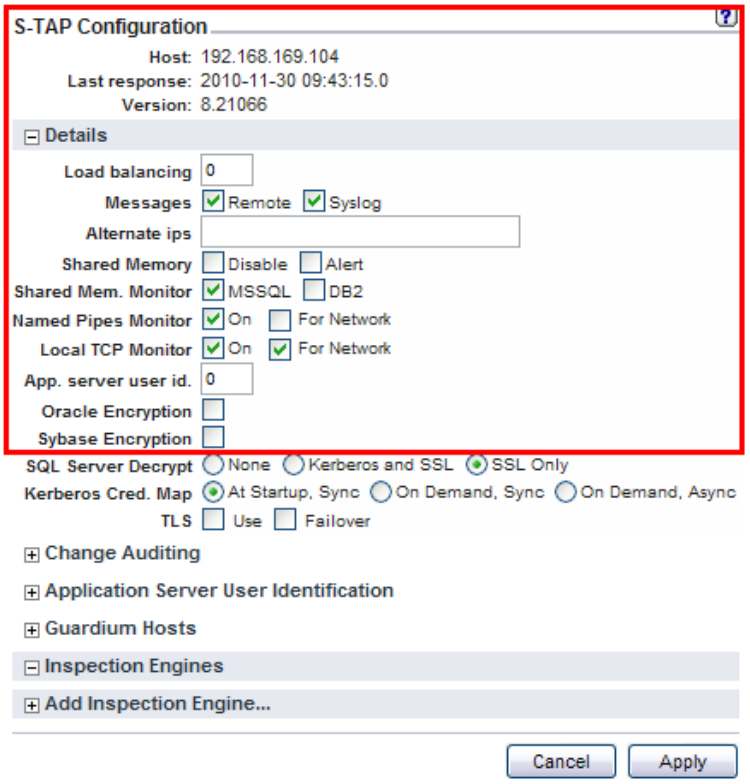
Click the **Edit** icon to configure S-TAP.

Note: S-Tap is running, but is not doing anything yet because there is no inspection engine configured.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP Configuration: Details (1 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 7-19. S-TAP Configuration: Details (1 of 2) GU2022.0

Notes:

The Details pane of the S-TAP Control panel applies to basic configuration settings for the S-TAP agent. The following describes Windows S-TAP controls:

- **Load balancing -** controls how S-TAP reports traffic to Guardium appliances, as follows:
  - 0 = Report all traffic to a single appliance (the default).
  - 1 = Load balancing; distribute sessions evenly to all appliances, by client port number (all traffic for a single session must go to the same appliance).
  - 2 = Full redundancy; report all traffic to all appliances.
- **Messages -** Controls where S-TAP processing messages (not database traffic) will be written: **Remote** writes the active Guardium host, **Syslog** writes to syslog file on the database server.
- **Shared Memory** - Controls the action to be taken when a shared memory connection is detected: **Disable** disconnects the session, **Alert** sends an alert. Note, these settings are rarely changed.

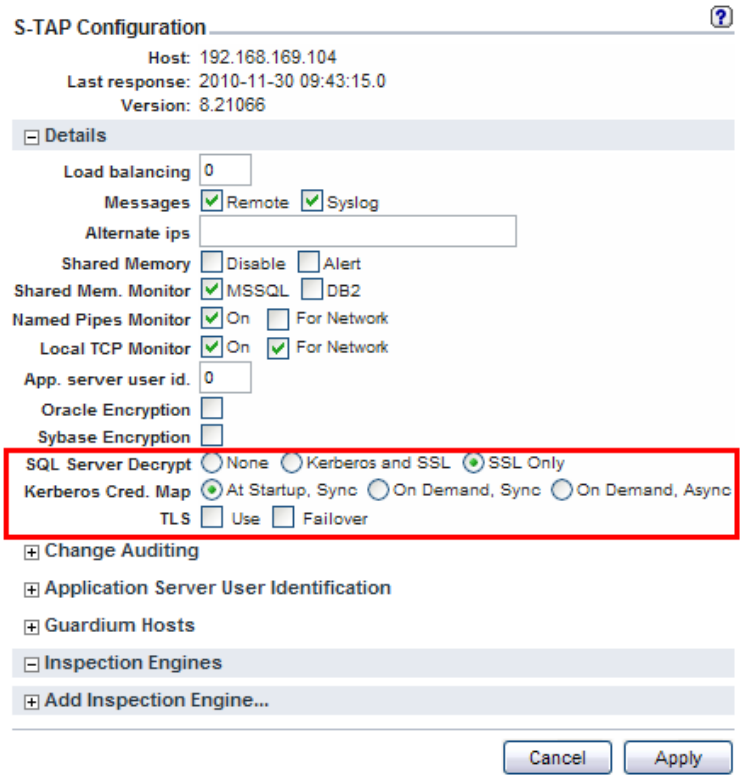
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Shared Mem. Monitor** – enable monitoring of shared memory
- **Named Pipes Monitor** – enable monitoring of named pipes traffic (both local and network)
- **Local TCP Monitor -** enable monitoring of TCP traffic (local and network)
- **App. Server user id. –** used for monitor application user names
- **Oracle Encryption –** monitor encrypted Oracle traffic
- **Sybase Encryption -** monitor encrypted Sybase traffic

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

S-TAP Configuration: Details (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 7-20. S-TAP Configuration: Details (2 of 2) GU2022.0

Notes:

- **SQL Server Decrypt -** Controls the type of automatic decryption applied to the traffic seen by S-TAP:
  - **None** - No automatic decryption. All SQL in SSL traffic will be ignored. All SQL in Kerberos traffic will be seen, but the database user name will be replaced by a string of hexadecimal characters (by Kerberos).
  - **Kerberos and SSL -** Automatically decrypts SSL and maps Kerberos names.
  - **SSL Only** Automatically decrypts SSL traffic. Use this option if all traffic of interest is SSL traffic. In this situation, even if Kerberos authentication is also used, it is of no consequence, because S-TAP obtains all of the information it needs before the message is encrypted, and before Kerberos replaces the real database username.
- **Kerberos Cred. Map –** When Kerberos authentication is used, controls how S-TAP obtains the database user names. If either Sync option (below) is selected, S-TAP will not forward messages to the Guardium appliance until it resolves the real database user name. When the Async option is used, all messages will be forwarded to the

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Guardium appliance, but initial sessions for users with new Kerberos tickets will have strings of hexadecimal characters in the database username field until S-TAP resolves the actual database user name.

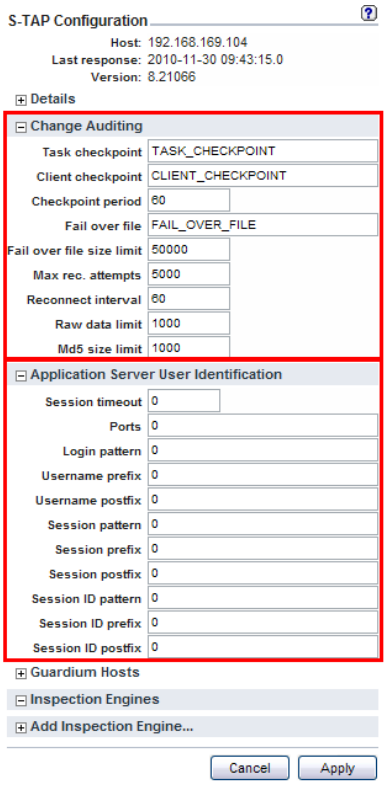
- **At Startup**, **Sync -** During startup processing, S-TAP obtains all authenticated users from the domain controller. This can be time consuming. After all users have been obtained and tabled, S-TAP starts sending data to the Guardium appliance. When it encounters a message from a user it does not recognize, it obtains that database user name as described for *On Demand, Sync, below.*
- **On Demand, Sync -** When S-TAP encounters a Kerberos message for an unrecognized user, S-TAP fetches the user name from the domain controller. It does not forward any traffic from that user to the Guardium appliance until it has the actual database user name.
- **On Demand, Async -** Like the above option, except that messages are not held while waiting to obtain the database user name.

- **TLS**
  - **Use -** Mark to use a TLS (encrypted) connection. This applies to both the S-TAP and CAS agents. Before changing this setting, verify that the ports used for this purpose are not being blocked by a firewall between the server and the Guardium appliance. See the Guardium Port Requirements table in the S-TAP Overview.
  - **Failover** - Mark to indicate that if no TLS connection can be established, a non-TLS connection can be used.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP Configuration: CAS and Application Server User ID



© Copyright IBM Corporation 2011, 2013

Figure 7-21. S-TAP Configuration: CAS and Application Server User ID GU2022.0

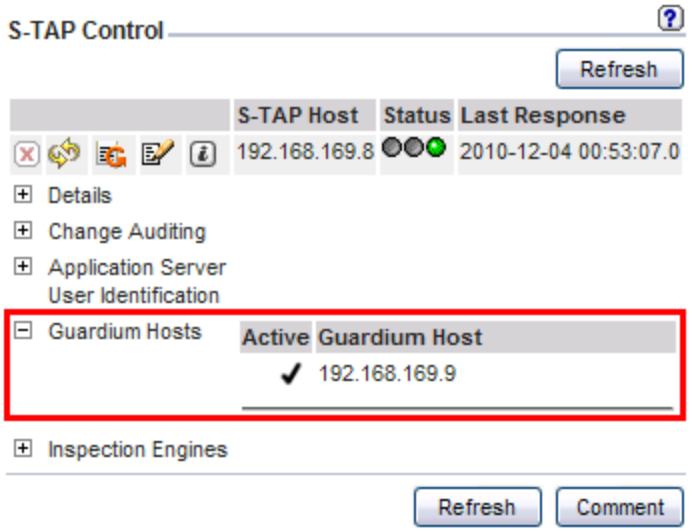
Notes:

Change Auditing – these settings will affect how CAS sends data to the collector. Generally, these should not be changed.

Application Server User Identification – this is used only when S-TAP is installed on the application server.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP Configuration: Guardium Hosts



© Copyright IBM Corporation 2011, 2013

Figure 7-22. S-TAP Configuration: Guardium Hosts GU2022.0

Notes:

This pane lists all Guardium appliances defined as hosts for the S-TAP. Additional hosts can be defined to provide a failover and load balancing capability. Guardium S-TAP hosts are referred to using three terms:

- **Active Host -** the host to which this S-TAP is currently connected. If you want to modify the S-TAP configuration from the Guardium administrator console, you must be logged into the active host. Usually, the active host will be the primary host.
- **Primary Host** - the preferred Guardium appliance to received data from (and control) this S-TAP. This is the host that the S-TAP attempts to connect with each time that the S-TAP restarts, or following a re-established the connection to primary host.
- **Secondary Host** - If multiple Guardium appliances are defined as hosts for the S-TAP, any appliance not designated as the primary host is a secondary host. If the S-TAP loses its connection to the active host, and it cannot re-connect to the primary host, it will attempt to connect to a secondary host, in the order listed. When you are logged into the administrator console of a secondary host, you can view the S-TAP

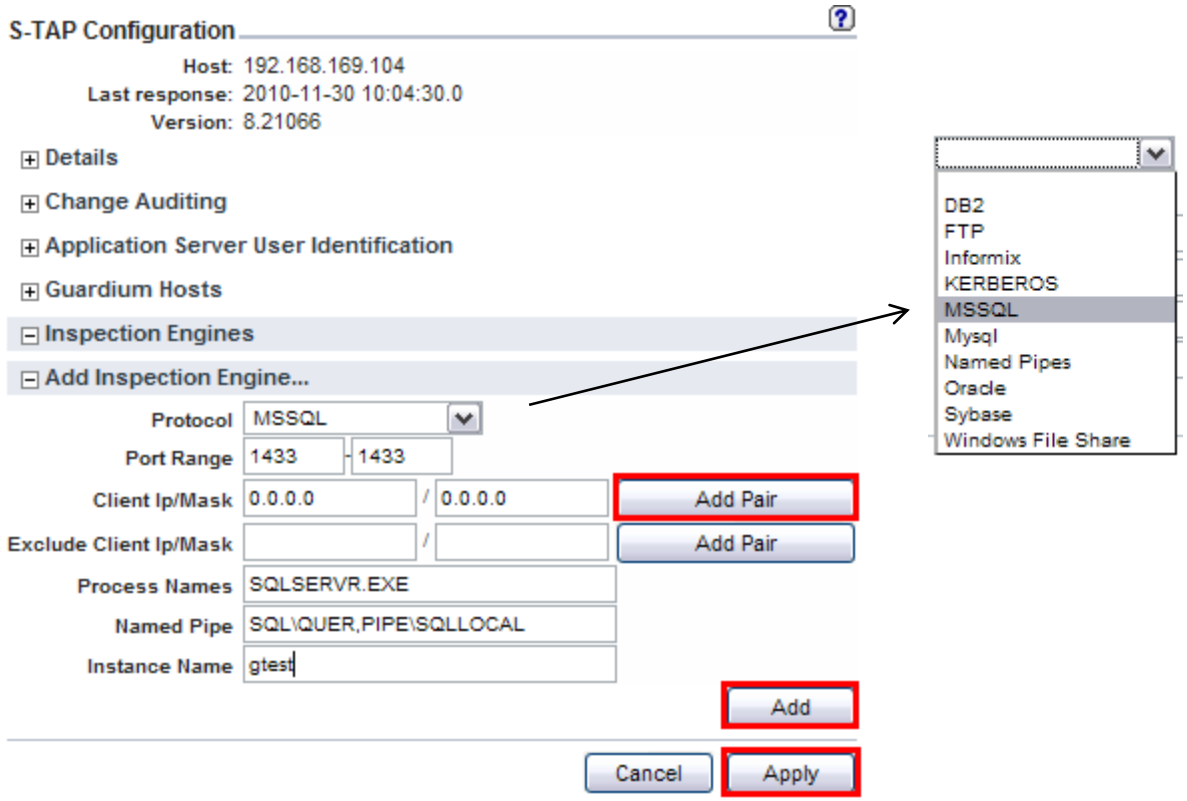
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

configuration, but you cannot edit it unless that host is also the active host at that moment.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Add Inspection Engines



© Copyright IBM Corporation 2011, 2013

Figure 7-23. Add Inspection Engines GU2022.0

Notes:

Inspection engines define what traffic on the database server will be forwarded to the collector. Fields for MS SQL on Windows include:

- **Protocol** - The type of database server being monitored (DB2, FTP, Informix, KERBEROS, MySQL, Netezza, Oracle, PostgreSQL, Sybase, Teradata, Windows File Share, etc.).
- **Port Range** - The range of ports monitored for this database server. There is usually only a single port in the range. If a range is used, do not include extra ports in the range, as this may result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.
- **Client IP/Mask** - A list of Client IP addresses and corresponding masks to specify which clients to monitor. If the IP address is the same as the IP address for the database server, and a mask of 255.255.255.255 is used, only local traffic will be monitored. An address/mask value of 1.1.1.1/0.0.0.0 (or 0.0.0.0/0.0.0.0) will monitor all clients.

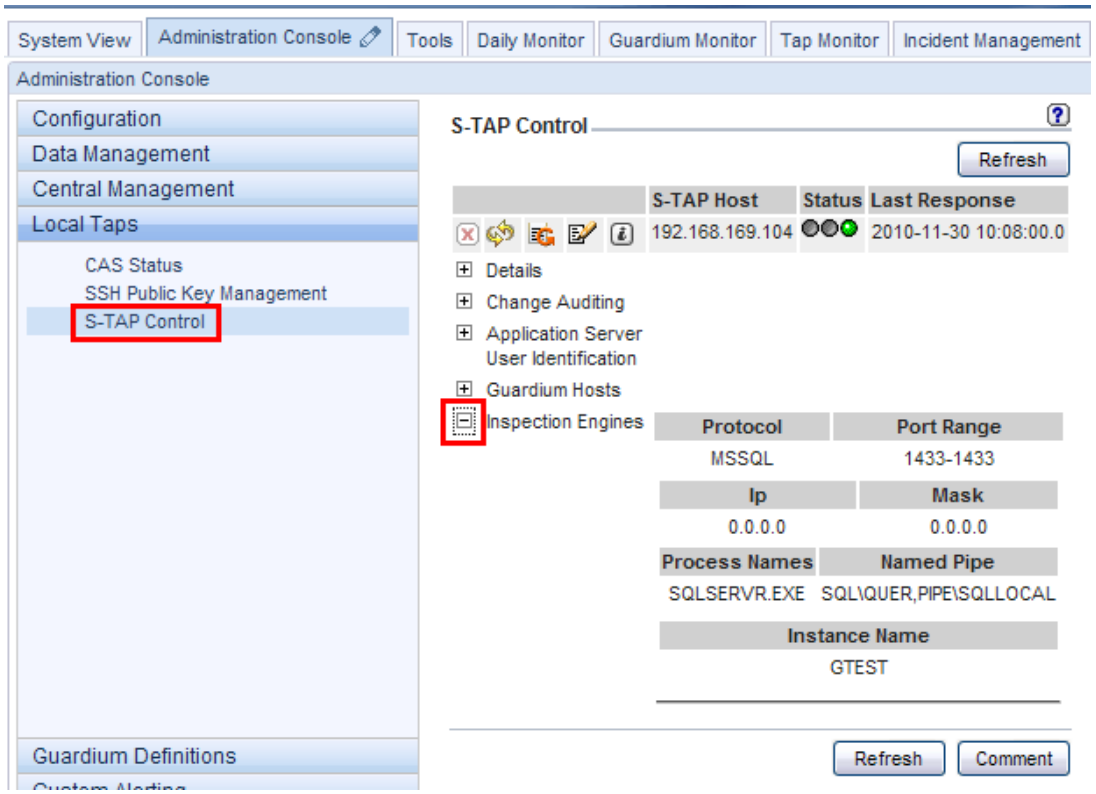
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Exclude Client IP/Mask** - A list of Client IP addresses and corresponding masks to specify which clients to exclude. This option allows you to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection of these).
- **Process Name** - For MS SQL Server use **sqlservr.exe**.
- **Named Pipes** - Specifies the name of the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified here, S-TAP will attempt to retrieve the named pipe name from the registry.
- **Instance Name**
  - The database instance name is required for: MS SQL Server 2005/2008 using encryption, or MS SQL Server using Kerberos Authentication (MSSQLSERVER is the default)

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Confirm Inspection Engine



© Copyright IBM Corporation 2011, 2013

Figure 7-24. Confirm Inspection Engine GU2022.0

Notes:

After you have made any changes to an inspection engine, always confirm that the changes are reflected in S-TAP Control. Go to **Administration Console -> Local taps -> S-TAP Control**. Expand **Inspection Engines** – your inspection engine should be listed.

Hint: Also check the System View pane. If the inspection engine is running, the S-TAP will be displayed in green and you will see numbers incrementing for the appropriate database server type.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Use the interactive installation method to setup S-TAP on a Windows database server
- Manually configure an Microsoft SQL Server inspection engine

© Copyright IBM Corporation 2011, 2013

Figure 7-25. Verify traffic GU2022.0

Notes:

Finally, confirm that the S-TAP is logging traffic successfully. You can use a report for this purpose.

Note: The Reports tab and the reports it contains are not out-of-the-box (OOTB). They were built separately in our Guardium environment.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GIM installation: UNIX/Linux

After completing this topic, you should be able to:

- Install the Guardium Installation Manger (GIM)
- Use GIM install to installed S-TAP on a Linux database server
- Install the Discovery module
- Use the Discovery module to automatically configure an inspection engine

© Copyright IBM Corporation 2011, 2013

Figure 7-26. Topic summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

7.2. GIM installation: UNIX/Linux

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GIM overview

- GIM
  - Guardium Installation Manager
- Gim Supervisor
  - Supervises Guardium processes

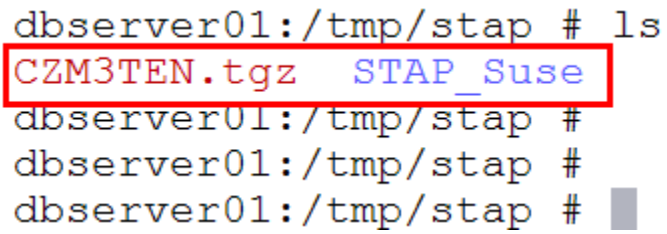
© Copyright IBM Corporation 2011, 2013

Figure 7-27. GIM installation: UNIX/Linux GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Download and extract GIM installer



© Copyright IBM Corporation 2011, 2013

Figure 7-28. GIM overview GU2022.0

Notes:

In the previous example, we used the interactive installation method to install S-TAP on Windows. A similar process is available for Unix, and is well documented in the S-TAP help book and the S-TAP checklist. The Guardium Installation Method (GIM) is a newer method, available since version 8.0, that will allow you to more easily install and maintain S-TAP. GIM is available for both Unix and Windows.

GIM is made of two components:

- **GIM** - responsible for such duties as registering to the GIM server, initiating a request to check for software updates, installing the new software, updating module parameters, and uninstalling modules.
- **GIM Supervisor** - responsible for starting, stopping, and making sure all of Guardium processes are running at all times and restarting them if they fail.

The GIM and GIM Supervisor processes can communicate with a collector or a Central Manager.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GIM installers directory

```
dbserver01:/tmp/stap # cd STAP_Suse/Discovery_and_GIM_Agents/
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents #
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents #
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents # ls
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-10-linux-i686.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-10-linux-ppc64.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-10-linux-x86_64.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-11-linux-i686.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-11-linux-x86_64.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-9-linux-i686.gim
guard-bundle-DISCOVERY-guard-8.0.xx_r20992_1-suse-9-linux-x86_64.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-i686.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-i686.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-ppc64.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-ppc64.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-x86_64.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-x86_64.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-11-linux-i686.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-11-linux-i686.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-11-linux-x86_64.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-11-linux-x86_64.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-9-linux-i686.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-9-linux-i686.gim.sh
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-9-linux-x86_64.gim
guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-9-linux-x86_64.gim.sh
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents #
```

© Copyright IBM Corporation 2011, 2013

Figure 7-29. Download and extract GIM installer GU2022.0

Notes:

In this example, we will install GIM and Discovery on a SUSE Linux database server running DB2. We will GIM to do the installation. We will also use the Instance discovery module to automatically configure inspection engines. Please note that, like Windows, you may also run the S-TAP installer and add inspection engines manually.

First, download the installer from IBM and extract it on the database server. In the example above the directory *STAP_Suse* was extracted from the file *CZM3TEN.tgz* using the command **tar –xzvf CZM3TEN.tgz**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Installing GIM

```
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents # mkdir /usr/gim
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents # ./guard-bundle-G
IM-guard-8.0.xx_r20992_1-suse-10-linux-i686.gim.sh -- --dir /usr/guardium/
 --sqlguardip 192.168.169.9 --tapip 192.168.169.8
```

```
related to any such action lapse.
d.      Each party waives any right to a jury trial in any proceeding arising ou
t of or related to this Agreement.

Installing modules ....
Installation completed successfully
dbserver01:/tmp/stap/STAP Suse/Discovery and GIM Agents #
```

```
dbserver01:/tmp/stap/STAP_Suse/Discovery_and_GIM_Agents # ps -ef |grep guard
root      7024     1  0 08:49 ?        00:00:00 /usr/bin/perl /usr/guardium/modu
les/GIM/8.0_r20992_1-1291211388/gim client.pl
root      7062  7024  0 08:49 ?        00:00:00 ../../perl ./guard_gimd.pl
root      7260     1  0 08:49 ?        00:00:00 /usr/guardium/modules/perl /usr/
guardium/modules/SUPERVISOR/8.0_r20992_1-1291211390/guard supervisor
```

```
dbserver01:/etc # tail -5 /etc/inittab

# end of /etc/inittab
fmc:2345:respawn:/opt/ibm/db2/V9.7/bin/db2fmcd #DB2 Fault Monitor Coordinator
gim:2345:respawn:/usr/bin/perl /usr/guardium/modules/GIM/8.0_r20992_1-1291211388
/gim_client.pl
gsvr:2345:respawn:/usr/guardium/modules/perl /usr/guardium/modules/SUPERVISOR/8.
0_r20992_1-1291211390/guard_supervisor
dbserver01:/etc #
```

© Copyright IBM Corporation 2011, 2013

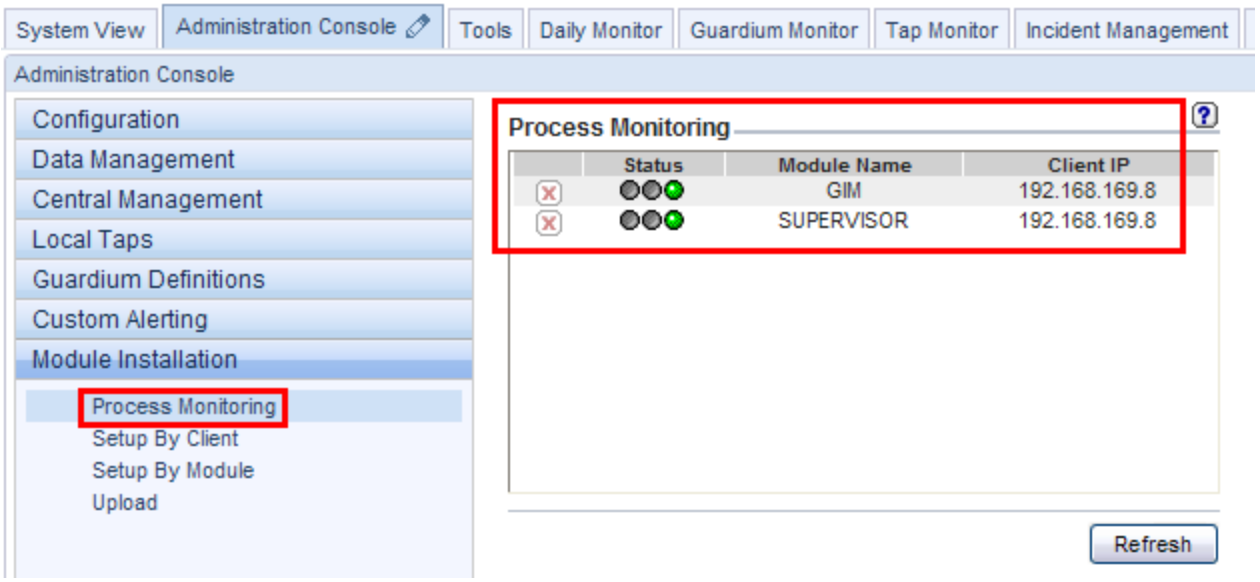
Figure 7-30. GIM installers directory GU2022.0

Notes:

Next, move to the *Disovery_and_GIM_Agents* directory, which will show you all of the GIM installers available for Suse Linux.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Confirm installation from the GUI



© Copyright IBM Corporation 2011, 2013

Figure 7-31. Installing GIM GU2022.0

Notes:

To install GIM, run the following command:

./guard-bundle-GIM-guard-<*OS Version*>.sh -- --dir <*install directory*> --sqlguardip <*collector or Central Manager IP address*> --tapip <*database server IP address*>

Note: The command is case and space sensitive!

In our example, we will be using the GIM installer for Suse 10 (i686) in the directory /usr/gim. The collector IP is 192.168.169.9 and the database server IP is 192.168.169.8. So our command will appear as follows:

./guard-bundle-GIM-guard-8.0.xx_r20992_1-suse-10-linux-i686.gim.sh -- --dir /**usr**/**gim**/ --sqlguardip **192.168.169.9** --tapip **192.168.169.8**

After running this command, scroll through the licensing agreement and, if the installation was successful, you will see the following messages:

Installing modules …

Installation completed successfully

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The database server will now have two new running processes – **gim_client.pl** and **guard_supervisor**, which can be viewed using the following Unix/Linux command:

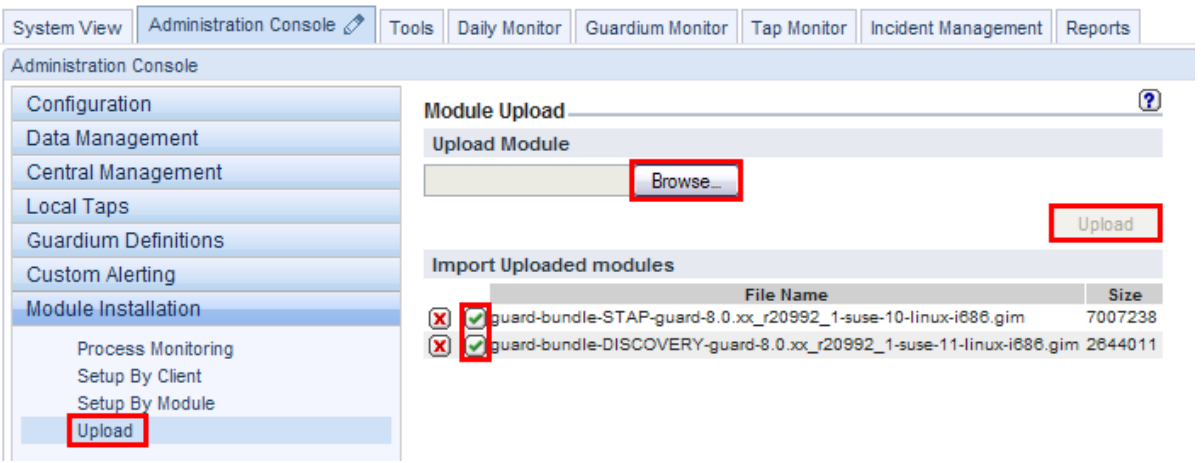
ps –ef |grep guard

To prevent any gaps in the audit data, GIM is maintained by the Unix/Linux *init* process, so there will be two new entries in the /etc/inittab file. These entries can be viewed using the following Unix/Linux command:

tail -5 /etc/inittab.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Module Upload



© Copyright IBM Corporation 2011, 2013

Figure 7-32. Confirm installation from the GUI GU2022.0

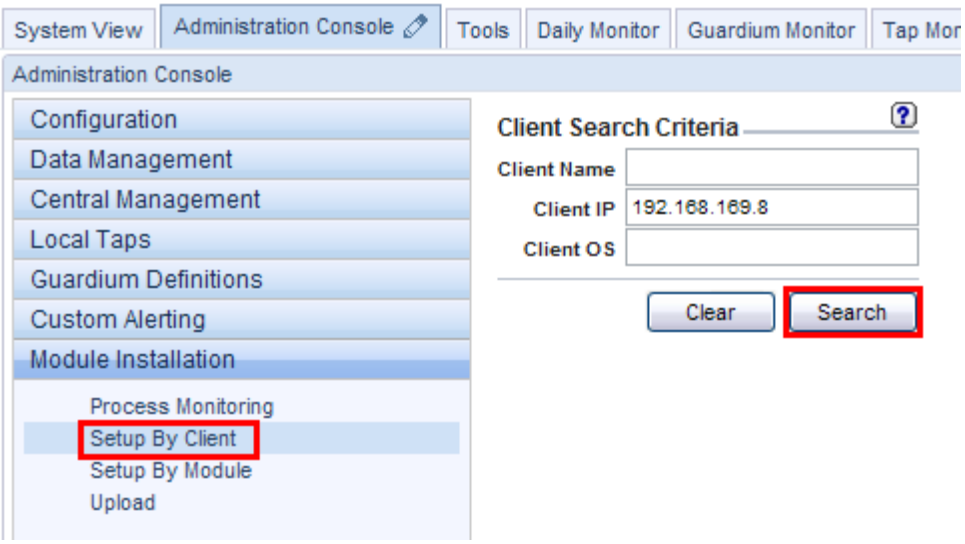
Notes:

After successfully completing the GIM installation, go the Guardium GUI and click the **Process Monitoring** link under **Administration Console** > **Process Monitoring**. You should have a GIM process and a SUPERVISOR process running on your database server. In this example GIM is pointed to a collector. GIM can also be managed by a Central Manager.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Setup By Client



© Copyright IBM Corporation 2011, 2013

Figure 7-33. Module Upload GU2022.0

Notes:

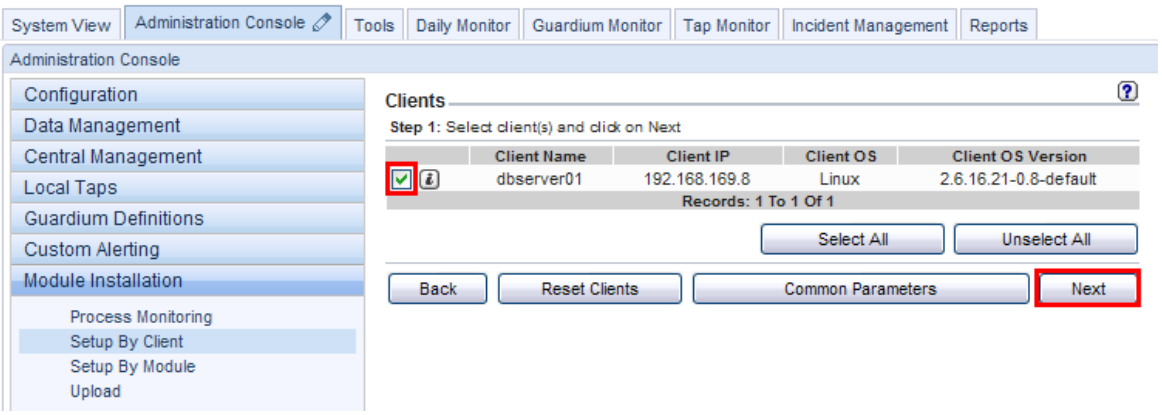
GIM is now available to aid in the installation of additional modules.

To apply modules, such as S-TAP, they must first be uploaded to the collector or Central Manager. To upload a module:

- Go to the **Upload** link under **Administration Console** > **Module Installation**
- Press **Browse** and locate the file
- Press **Upload**
- Repeat the above steps for all of the files which you would like to upload
- Press the *check* icon for each of the uploaded files

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Select clients



© Copyright IBM Corporation 2011, 2013

Figure 7-34. Setup By Client GU2022.0

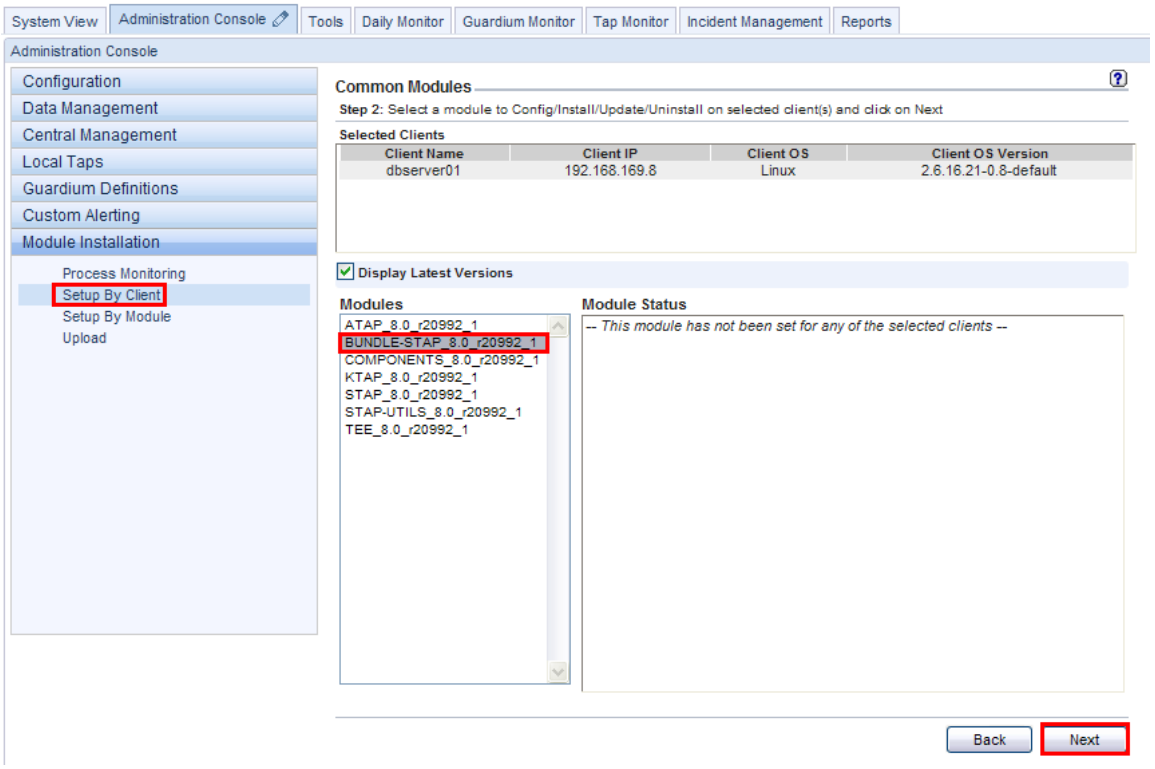
Notes:

The next step is to apply the S-TAP Bundle to the client. Click the **Setup By Client** link and press **Search**. Optionally, you may filter the search by Client Name, Client IP or Client OS.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Common modules



© Copyright IBM Corporation 2011, 2013

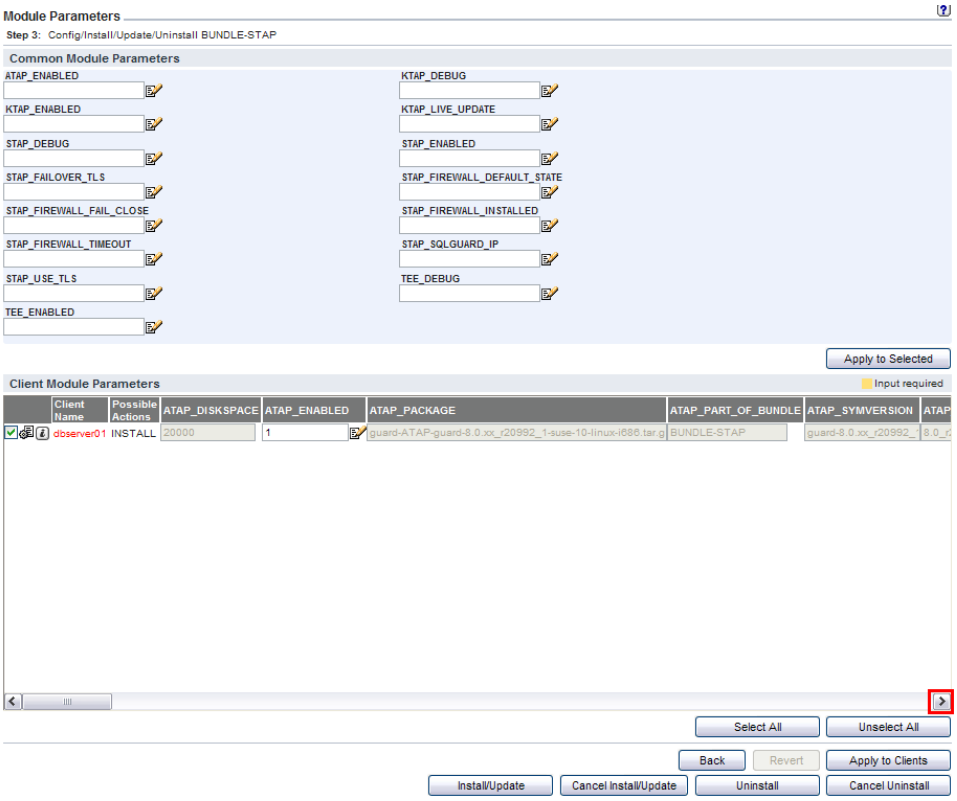
Figure 7-35. Select clients GU2022.0

Notes:

Step 1 - Check the box(es) for the database server(s) for which you would like to apply the module and press **Next**. If you have multiple servers, you may choose more than one from this screen.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Module Parameters



© Copyright IBM Corporation 2011, 2013

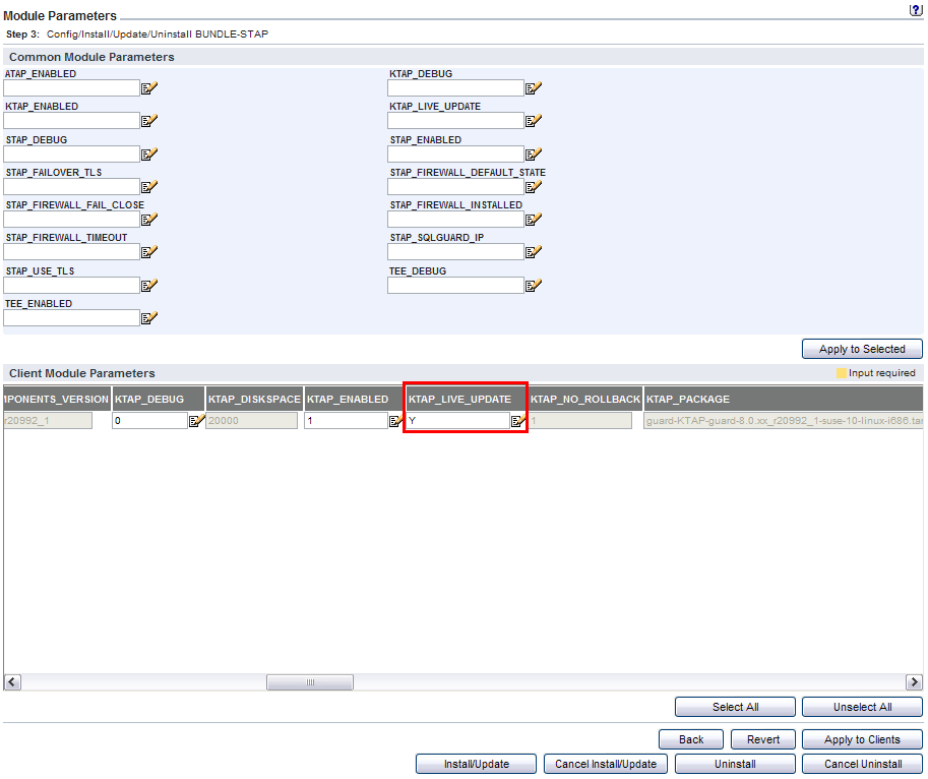
Figure 7-36. Common modules GU2022.0

Notes:

Step 2 - High light the module that you would like to install and press **Next**. In general, you should choose to install bundles rather than individual components, such as STAP & KTAP.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Client Module Parameters (1 of 2)



© Copyright IBM Corporation 2011, 2013

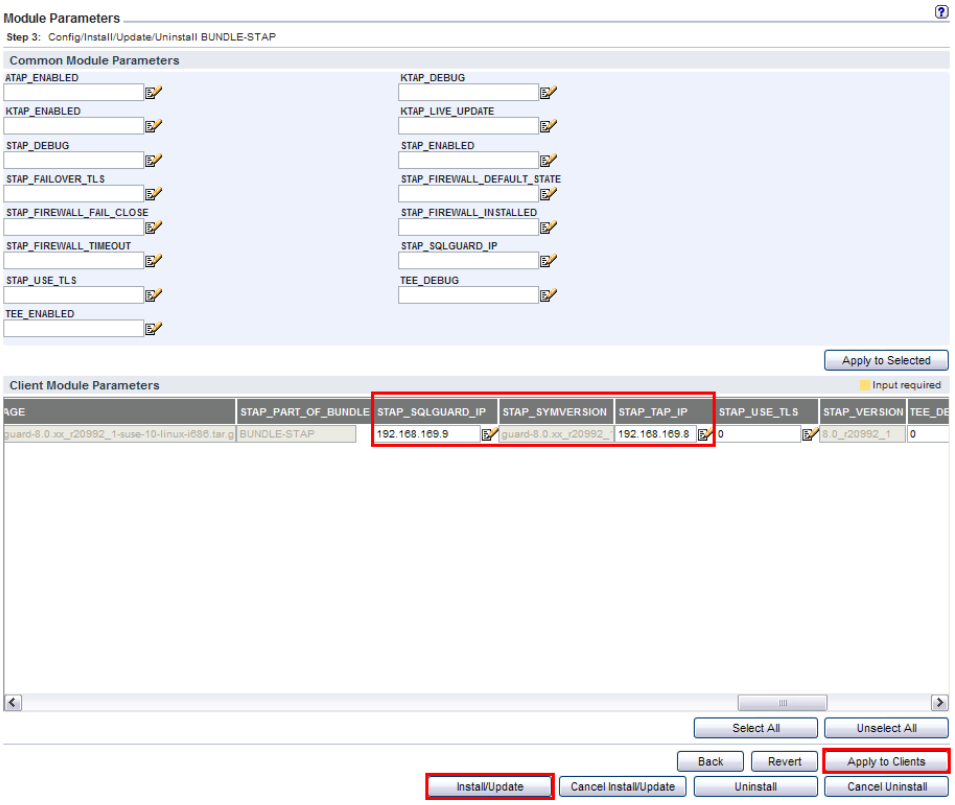
Figure 7-37. Module Parameters GU2022.0

Notes:

Step 2 - The *Module Parameters* allows you to apply the S-TAP settings. The **Common Module Parameters** pane would apply toward all of GIM clients chosen in Step 1, if you had selected multiple database servers. In this example, we only chose one module, so we will only be changing the settings under **Client Module Parameters**. Scroll to the right to the select the appropriate settings.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Client Module Parameters (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 7-38. Client Module Parameters (1 of 2) GU2022.0

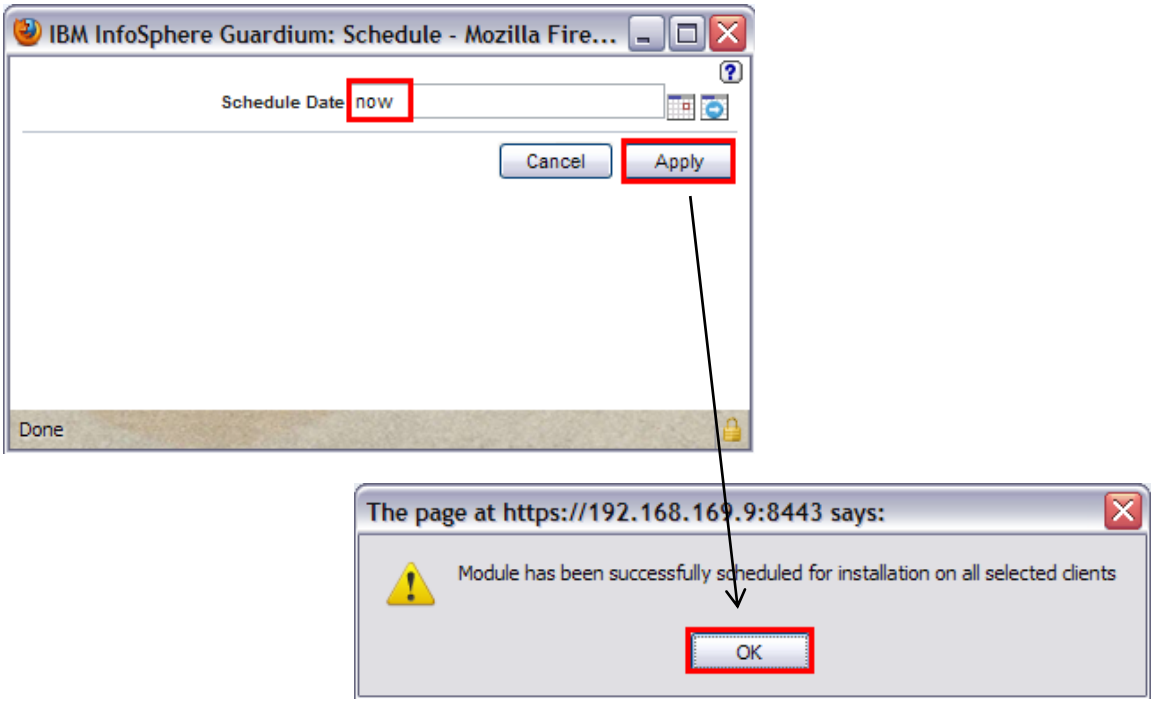
Notes:

Step 3 continued – For Unix, the first setting we will apply is changing **KTAP_LIVE_UPDATE** to **Y**. In Unix and Linux, this will later allow you to upgrade S-TAP without rebooting the database server.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Schedule installation



© Copyright IBM Corporation 2011, 2013

Figure 7-39. Client Module Parameters (2 of 2) GU2022.0

Notes:

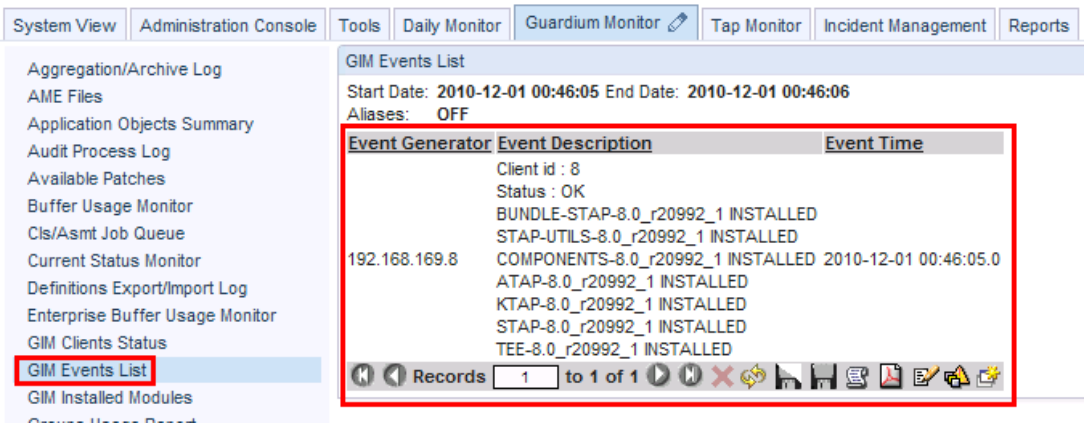
Step 3 continued - Continue to scroll to the right and make the following entries:

- **STAP_SQLGUARD_IP** = the IP address of the collector. If you are running this process from a Central Manager, this could include any of the managed units. In this case we are running it from a collector, so the IP address will be the same as the collector we are using, which is **192.168.169.9**.
- **STAP_TAP_IP** = the IP address of the database server, which is **192.168.169.8**.

After making these entries, press **Apply to Clients** and **Install/Update** to complete the configuration.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GIM Events List



© Copyright IBM Corporation 2011, 2013

Figure 7-40. Schedule installation GU2022.0

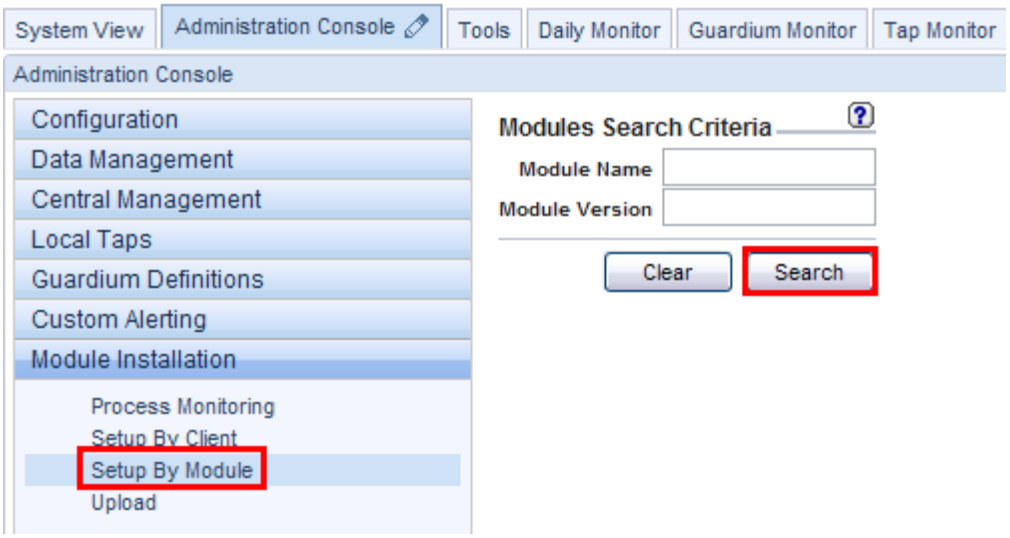
Notes:

After pressing ‘Install/Update’, a scheduling window will appear. Enter the time that you would like to install to run and press apply. In this example, we will enter **Now** to run the installation immediately.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Discovery Setup By Module



© Copyright IBM Corporation 2011, 2013

Figure 7-41. GIM Events List GU2022.0

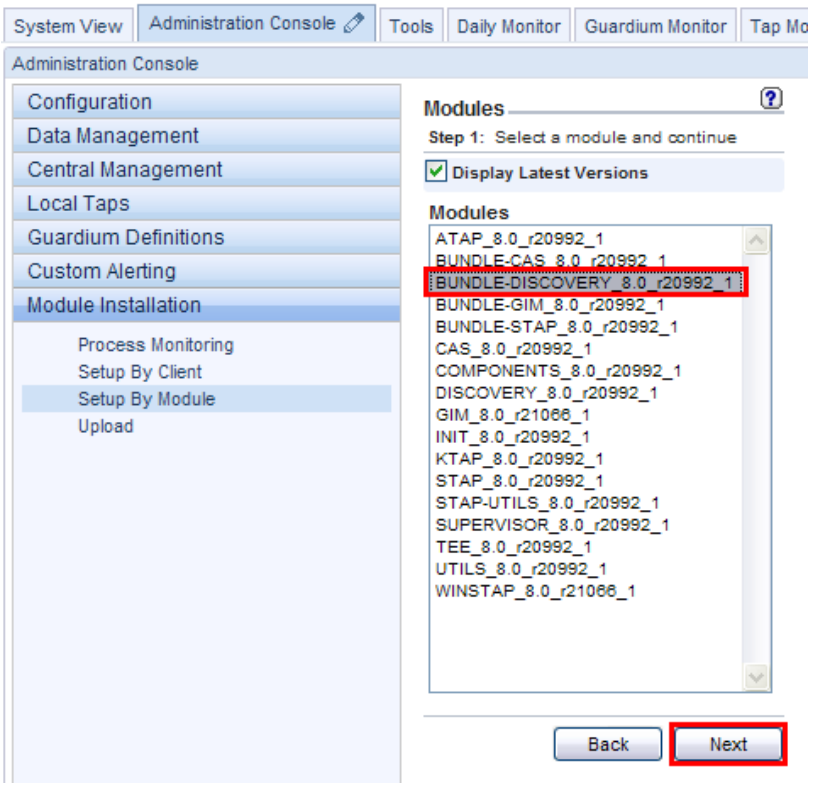
Notes:

It will take a few minutes for the process to complete. You can check the **GIM Events List**, which can be found on the Guardium Monitor table, to check the status.

Hint: The GIM Installed Modules option will also come in handy to verify the modules which were GIM installed.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Bundle-discovery



© Copyright IBM Corporation 2011, 2013

Figure 7-42. Discovery Setup By Module GU2022.0

Notes:

Next we will install the **Discovery** module, which, after it is installed, will search for database instances on your server and allow you to quickly create inspection engines based on those discovered instances.

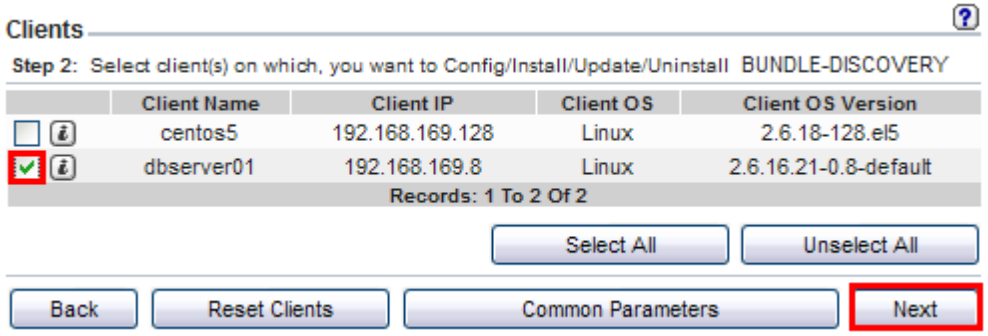
In this example, we will use **Setup By Module** as follows

- Go to **Administration Console** > **Module Installation** and click **Setup By Module**
- Press the **Search** button

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Select client



© Copyright IBM Corporation 2011, 2013

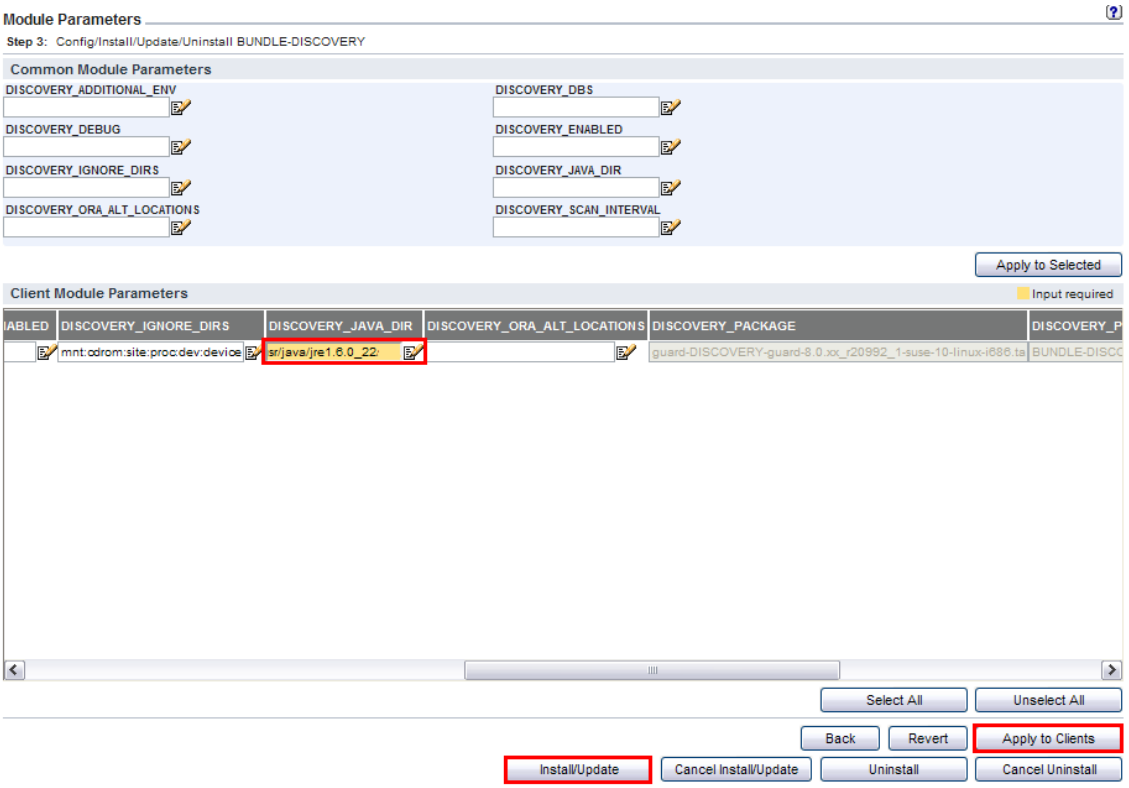
Figure 7-43. Bundle-discovery GU2022.0

Notes:

Highlight the **BUNDLE-DISCOVERY…** module from the list and press **Next**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Java installation directory



© Copyright IBM Corporation 2011, 2013

Figure 7-44. Select client GU2022.0

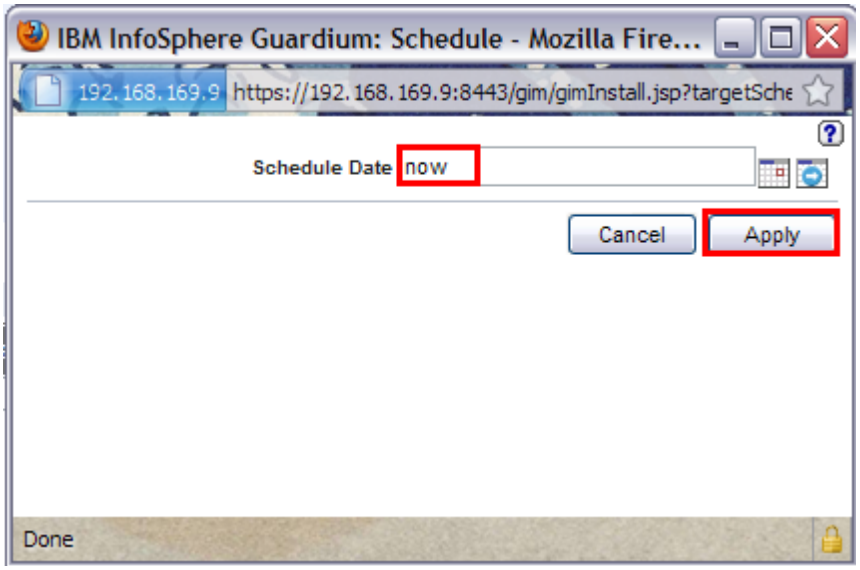
Notes:

Select the database server(s) on which you would like to install the module and press **Next**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Schedule installation



© Copyright IBM Corporation 2011, 2013

Figure 7-45. Java installation directory GU2022.0

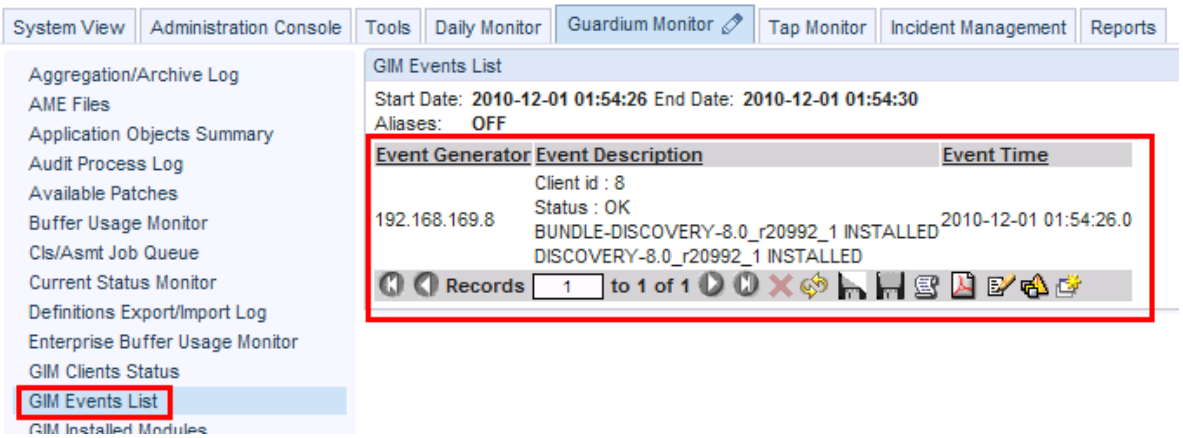
Notes:

Again, there will be Common Module Parameters and Client Module Parameters.

Scroll over to the **DISCOVERY_JAVA_DIR** field and enter location of Java installation directory on the database server (for example */usr/java/jre1.6.0_22*). Java is required to run this module. After entering the java installation directory press **Apply to Clients** and **Install/Update**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GIM Events List



© Copyright IBM Corporation 2011, 2013

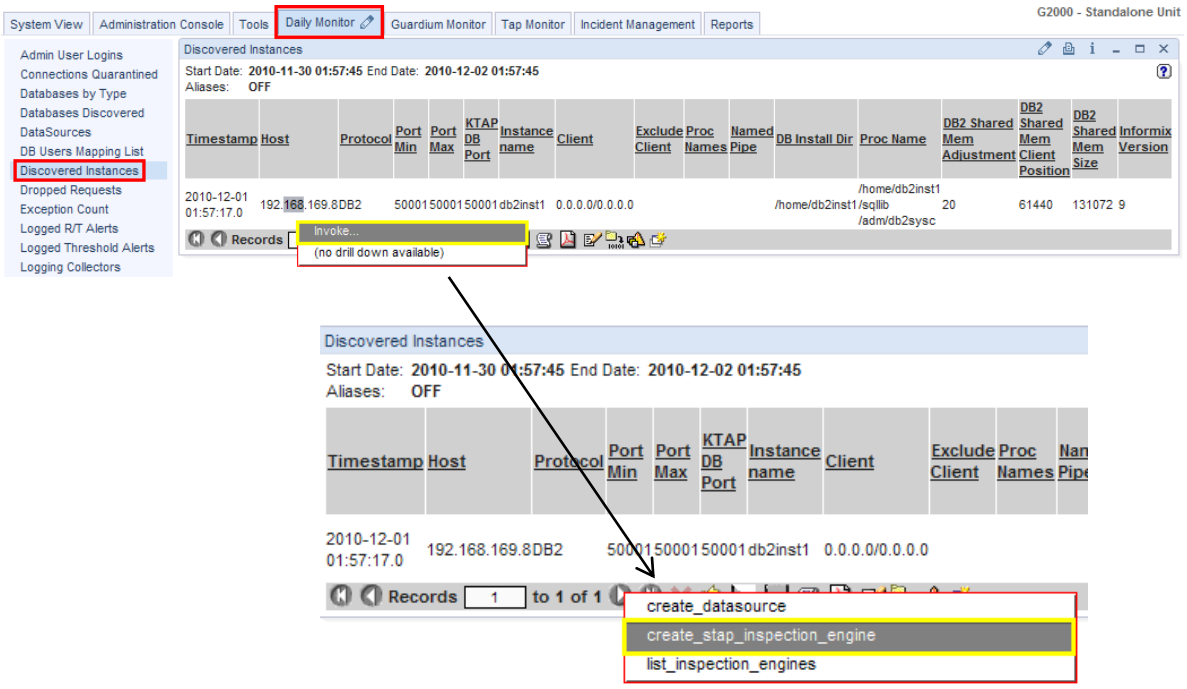
Figure 7-46. Schedule installation GU2022.0

Notes:

In *Schedule Date* enter **now** and press the **Apply** button.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Create S-TAP inspection engine



© Copyright IBM Corporation 2011, 2013

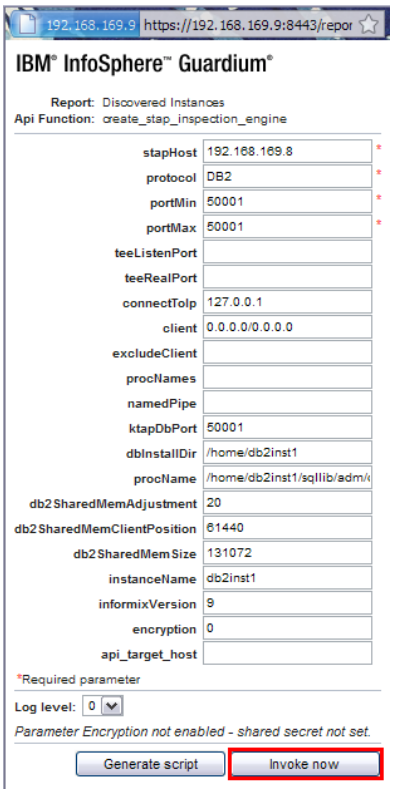
Figure 7-47. GIM Events List GU2022.0

Notes:

To confirm that the Discover module has installed successfully, go to the **Guardium Monitor** tab and click the **GIM Events List**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Invoke now



© Copyright IBM Corporation 2011, 2013

Figure 7-48. Create S-TAP inspection engine GU2022.0

Notes:

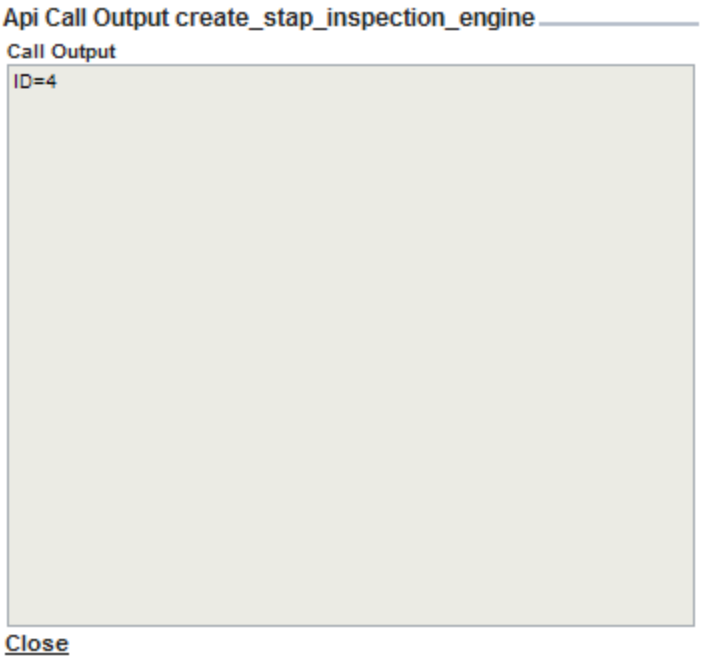
To view any instances found by the Discovery module, go to **Daily Monitor** and click the **Discovered Instances** link. From here you can also quickly create an S-TAP inspection engine based on any newly discovered instance. To create a new inspection engine:

- In the report Double click in the line of the instance on which you would like to create an inspection engine and choose **Invoke…**
- Then choose **create_stap_inspection_engine**

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Complete process



© Copyright IBM Corporation 2011, 2013

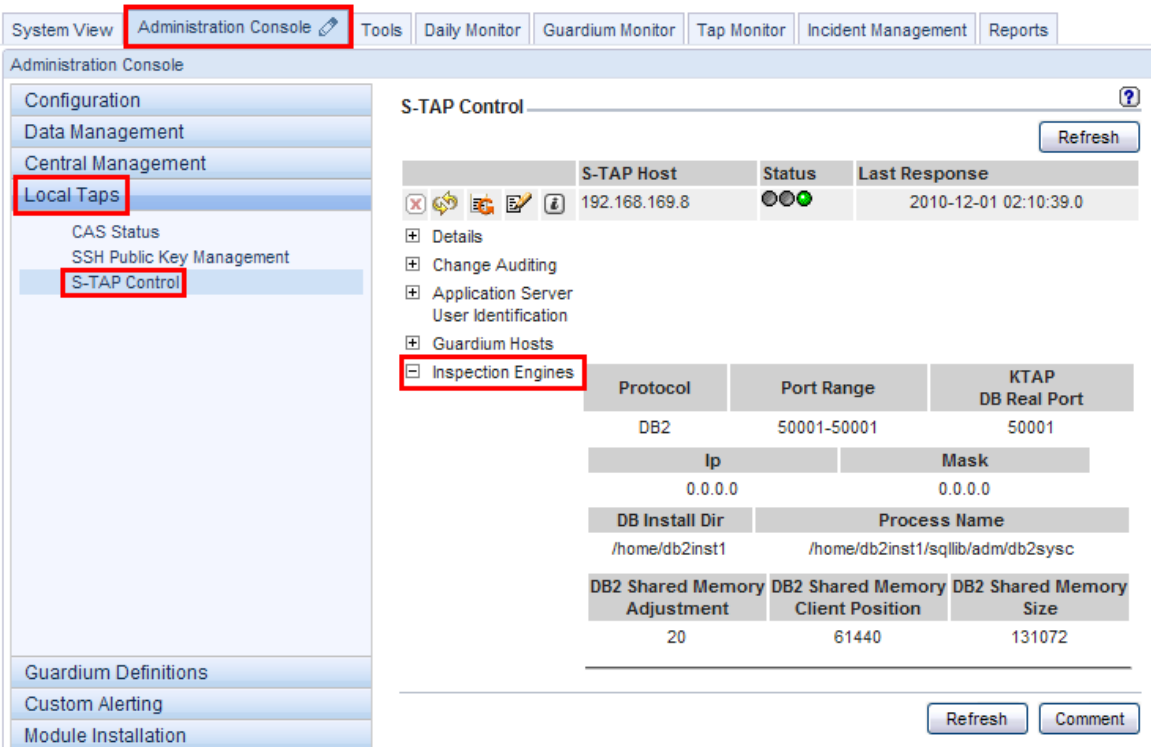
Figure 7-49. Invoke now GU2022.0

Notes:

On the next screen confirm that the settings appear correct and press **Invoke now**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Confirm Inspection Engine creation



© Copyright IBM Corporation 2011, 2013

Figure 7-50. Complete process GU2022.0

Notes:

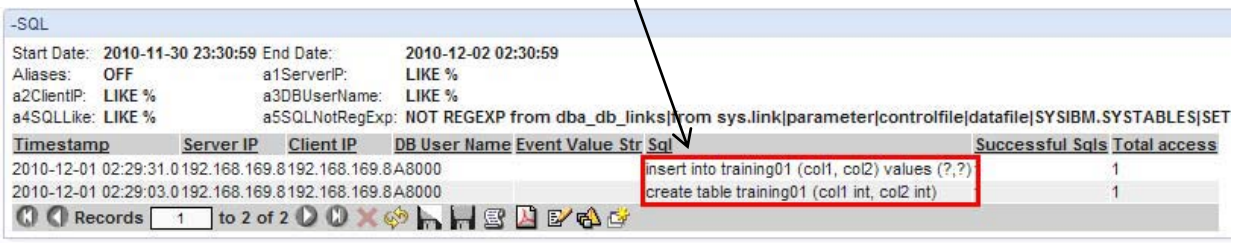
Press **Close** after the process completes

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Verify traffic

```
db2 => connect to localtcp user a8000 using a8000abc

   Database Connection Information

 Database server        = DB2/LINUX 9.7.1
 SQL authorization ID   = A8000
 Local database alias   = LOCALTCP

db2 => create table training01 (col1 int, col2 int)
DB20000I  The SQL command completed successfully.
db2 => insert into training01 (col1, col2) values (12929,484)
DB20000I  The SQL command completed successfully.
```



© Copyright IBM Corporation 2011, 2013

Figure 7-51. Confirm Inspection Engine creation GU2022.0

Notes:

Next, go to **Administration Console** > **Local Taps** > **S-TAP Control** and click the **Inspection Engines** button to confirm that the inspection engine was created correctly.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Install the Guardium Installation Manger (GIM)
- Use GIM install to installed S-TAP on a Linux database server
- Install the Discovery module
- Use the Discovery module to automatically configure an inspection engine

© Copyright IBM Corporation 2011, 2013

Figure 7-52. Verify traffic GU2022.0

Notes:

Finally, confirm that the collector is capturing traffic. The System View pane can be used for this verification, as can various reports.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-TAP installation: Non-interactive methods

After completing this topic, you should be able to:

- Understand the non-interactive installation methods for UNIX and Linux
- Understand how to use GuardAPI to configure inspection engines

© Copyright IBM Corporation 2011, 2013

Figure 7-53. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

7.3. S-TAP installation: Non-interactive methods

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

UNIX non-interactive installer

guard-stap-setup [--modules <module-bundles>] [--ni] [--tls <0|1>|-k|-t|--dir <dir>|--tapip <tapip>|--sqlguardip <sqlguardip>|--tapfile <file>] [--presets <presets-file> | <preset-option-list>...]

© Copyright IBM Corporation 2011, 2013

Figure 7-54. S-TAP installation: Non-interactive methods GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Windows non-interactive installer

setup /s /z"<key>;<install_dir>;<install_table_file>;<options>“

Example:
Assume that the following configuration table file:
\\192.168.1.201\shareFolder\stap_configuration

Contains the following two entries (hostname, IP, Guardium Appliance):
raven 192.168.2.20 192.168.3.113
seagull 192.168.2.22 192.168.3.113

The following command (with no line breaks) can be used to install S-TAP on the raven server (192.168.2.20). Please note that the actual command contains no line breaks:

setup /s /z"raven;c:\program files\guardium\guardium_stap;
\\192.168.1.201\shareFolder\stap_configuration;
MSSQLSharedMemory=1 DB2SharedMemory=1 CAS=1 NamedPipes=1
Lhmon=1 LhmonForNetwork=1 TLS=1 START=1"

© Copyright IBM Corporation 2011, 2013

Figure 7-55. UNIX non-interactive installer GU2022.0

Notes:

Below is the syntax to configure the Unix non-interactive installer:

<guard-stap-setup> is the name of the script file.

- **--modules** is the tgz file with all the compiled kernel modules
- **--ni** indicates that the shell is being run in non-interactive mode.
- **--tls** specifies that the S-TAP and collector communication is in TLS protocol with failover more 0 or 1.
  - 0 - do not failover. If fails to connect to collector, keep on trying using TLS.
  - 1 - failover to non-tls protocol, if fails to connect to collector, failover to non-secure protocol
- **-k** indicates that K-Tap should be installed, or
- **-t** indicates that the Tee should be installed.
- **--dir <s-tap_dir>** identifies the S-TAP installation directory

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **--tapip <ip_address>** specifies the IP address of the database server. Omit if --tapfile is used.
- **--sqlguardip<guardium_ip>** specifies the IP address of the Guardium appliance. Omit if --tapfile is used.
- **--tapfile <file>** identifies a text file listing one or more servers on which the S-TAP agent is to be installed. Each row of the text **file must** have the following format, with each of the following three variables separated from the next by a tab character: <hostname> <tap_ip> <sqlguard_ip>, where hostname is the name of the database server, tap_ip is the IP address of the database server, and sqlguard_ip is the IP address of the Guardium appliance.
- **--presets** may be a file that contains a subset of global guard_tap.ini options or an option list

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

GrdApi inspection engine creation

The GuardAPIs can be used to create and configure inspection engines:

grdapi create_stap_inspection_engine stapHost=192.168.2.118 protocol=Oracle portMin=1521 portMax=1521 dbInstallDir=/data/oracle10 procName=/data/oracle10/oracle/product/10.2.0/db_1/bin/oracle client=192.168.0.0/255.255.0.0 ktapDbPort=1521

© Copyright IBM Corporation 2011, 2013

Figure 7-56. Windows non-interactive installer GU2022.0

Notes:

Below is the syntax to configure the Windows non-interactive installer:

setup /s /z"<key>;<install_dir>;<install_table_file>;<options>“

- **key** - A string value used to identify a line in the install_table_file. There will be one line for each S-TAP. In addition to the key, the install table file must contain the following:
  - **server ip or hostname** - The IP address or host name of the database server on which S-TAP will be installed.
  - **guard ip or hostname** - The address or host name of the Guardium appliance to which this S-TAP will report.
- **install_dir** - Identifies the program directory into which the S-TAP agent will be installed.
- **install_table_file** - Full network path name of the install table file, which must be accessible from all database server machines on which S-TAP will be installed (from the command line). This must be a text file, with fields separated by spaces, and it must have Unix-format line separator characters (\n).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Options** – described below:
  - **MSSQLSharedMemory** - Install the MS SQL Server shared memory driver to monitor MS SQL Server traffic via shared memory.
  - **DB2SharedMemory** - Install the DB2 shared memory driver to monitor DB2 traffic via shared memory.1
  - **TLS** - Use a secure (encrypted) connection for all communication with the Guardium appliance.
  - **failoverTLS** - Applies only if TLS (above) is true. If no TLS connection can be made, attempt to connect over a non-secure connection.
  - **CAS** - Install the CAS agent. (It can be installed later, without having to uninstall or re-install S-TAP.)
  - **NamedPipes** - Install the Named Pipes driver to monitor local traffic over named pipes.
  - **Lhmon** - Install the LHmon driver to monitor local TCP traffic.
  - **LhmonForNetwork** - Use LHmon to monitor network TCP traffic.
  - **START** - Start the S-TAP and/or CAS service after installation.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

After completing this topic, you should be able to:

- Understand the non-interactive installation methods for UNIX and Linux
- Understand how to use GuardAPI to configure inspection engines

© Copyright IBM Corporation 2011, 2013

Figure 7-57. GrdApi inspection engine creation GU2022.0

Notes:

The syntax to create an inspection engine using GrdApi include the following (see the S-TAP help book for additional optional commands:

- **grdapi create_stap_inspection_engine** – the Guard API command
- **Protocol** - The database protocol (DB2, Informix, Oracle Sybase, MySQL, FTP, Windows file share, kerberos, MSSQL, Named Pipes
- **portMin** - Starting port number of the range of listening ports configured for the database.
- **portMax** - Ending port number of the range of listening ports for the database (see the note above).
- **Client** - A list of Client IP addresses and corresponding masks to specify which clients to monitor. A client address/mask value of 1.1.1.1/0.0.0.0 will monitor all clients.
- **procNames** - For a Windows Server: For Oracle or MS SQL Server only, when named pipes are used. For Oracle, the list usually has two entries: oracle.exe,tnslsnr.exe. For MS SQL Server, the list is usually just one entry: sqlservr.exe.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **namedPipe** - Windows only. Specifies the name of a named pipe. If a named pipe is used, but nothing is specified here, S-TAP retrieves the named pipe name from the registry.
- **ktapDbPort** - Under Unix, used only when the K-Tap monitoring mechanism is used. Identifies the database port to be monitored by the K-Tap mechanism.
- **dbInstallDir** - Unix only. Enter the full path name for the database installation directory. For example: /home/oracle10
- **procName** - For a Unix Server: For a DB2, Oracle, or Informix database, enter the full path name for the database executable.
- **instanceName** - Used only for MQSQL or Oracle encrypted traffic. Either the MSSQL or ORACLE encryption flag must be turned on before the this parameter can be used.

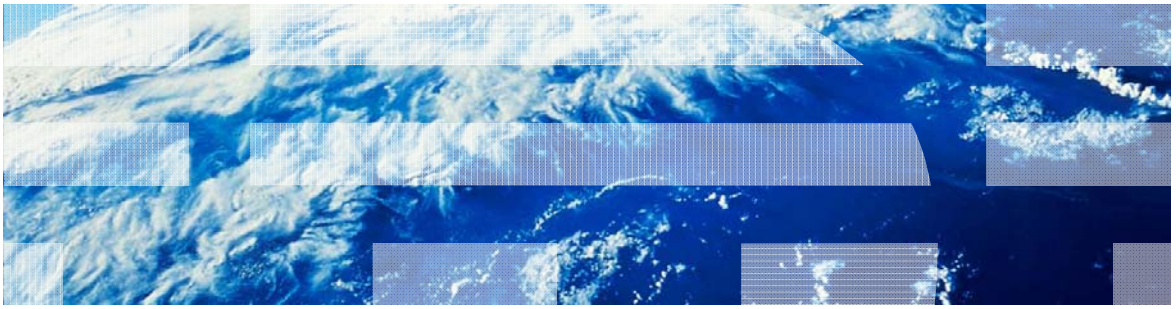
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

InfoSphere Guardium

Information Management software

S-TAP and GIM



© Copyright IBM Corporation 2011, 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6.0

Figure 7-58. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. An S-TAP is installed on and monitors traffic on a _____ server.

   a. Guardium
   b. Network
   c. DNS
   d. Database

2. List three ways an S-TAP can be installed.

3. There are two ways GIM can install additional modules, by _____ and by _____.

4. What is the difference between a Common Module Parameter and a Client Module Parameter?

5. True or false: GuardAPIs are designed to run in an executable script, and provide a method of performing non-interactive installs.

© Copyright IBM Corporation 2011, 2013

Figure 7-59. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. An S-TAP is installed on and monitors traffic on a _____ server.
   a. Guardium
   b. Network
   c. DNS
   d. **Database**

2. List three ways an S-TAP can be installed.

   Interactive S-TAP installer

   Guardium Installation Manager

   GuardAPI non-interactive installation

3. There are two ways GIM can install additional modules, by **client** and by **module**.

4. What is the difference between a Common Module Parameter and a Client Module Parameter?

   Common - Used when there are multiple database servers being configured at once; parameters apply to all of them. Client - Used when there is just one database server being configured; parameters apply to just that server.

5. True or false: GuardAPIs are designed to run in an executable script, and provide a method of performing non-interactive installs.

Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand S-TAP
- Install S-TAP on Windows interactively
- Install S-TAP on Linux using GIM
- Understand the non-interactive installation methods

© Copyright IBM Corporation 2011, 2013

Figure 7-60. Unit summary GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 4** in the Exercise Guide.

© Copyright IBM Corporation 2011, 2013

Figure 7-61. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution

1. An S-TAP is installed on and monitors traffic on a _____ server.

   a. Guardium
   b. Network
   c. DNS
   d. Database

2. List three ways an S-TAP can be installed.
   1. **Interactive S-TAP installer**
   2. **Guardium Installation Manager**
   3. **GuardAPI non-interactive installation**

3. There are two ways GIM can install additional modules, by **client** and by **module**.

© Copyright IBM Corporation 2011, 2013

Figure 7-62. Checkpoint solution GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution continued

4. What is the difference between a Common Module Parameter and a Client Module Parameter? **Common – Used when there are multiple database servers being configured at once; parameters apply to all of them. Client – Used when there is just one database server being configured; parameters apply to just that server.**

5. **True** or false: GuardAPIs are designed to run in an executable script, and provide a method of performing non-interactive installs.

© Copyright IBM Corporation 2011, 2013

Figure 7-63. Checkpoint solution continued GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 8. Group Builder

Estimated time

1:00

What this unit is about

This unit describes how to create and use groups.

What you should be able to do

After completing this unit, you should be able to:

- Understand all of the options to create groups
- Create groups using the manual entry and populate from query methods

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand all of the options to create groups
- Create groups using the manual entry and populate from query methods

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-1. Unit objectives GU2022.0

Notes:

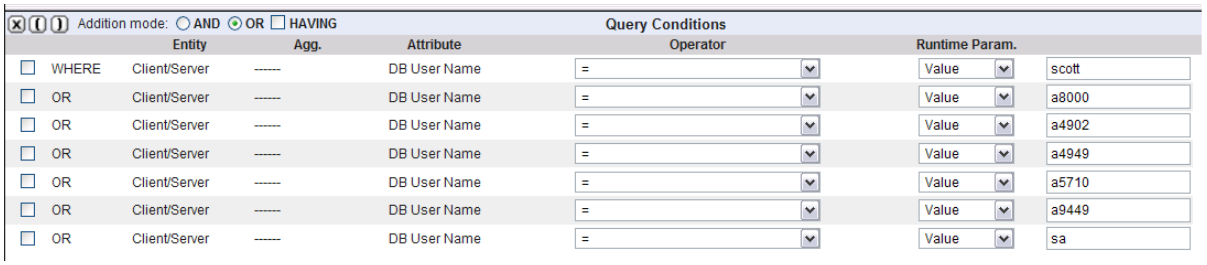
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Group: Definition

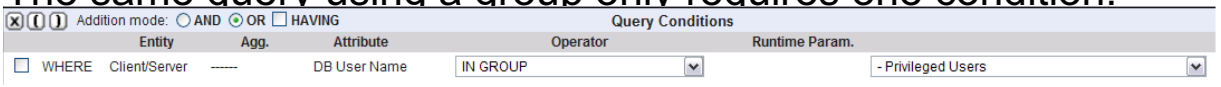
A **group** is a list of data elements.

Groups are used to facilitate the creation of queries and policy rules

A query without groups would require many ‘OR’ conditions!


Addition mode: AND OR HAVING
Query Conditions
Entity Agg. Attribute Operator Runtime Param.
WHERE Client/Server ------ DB User Name = Value scott
OR Client/Server ------ DB User Name = Value a8000
OR Client/Server ------ DB User Name = Value a4902
OR Client/Server ------ DB User Name = Value a4949
OR Client/Server ------ DB User Name = Value a5710
OR Client/Server ------ DB User Name = Value a9449
OR Client/Server ------ DB User Name = Value sa

The same query using a group only requires one condition.


Addition mode: AND OR HAVING
Query Conditions
Entity Agg. Attribute Operator Runtime Param.
WHERE Client/Server ------ DB User Name IN GROUP - Privileged Users

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-2. Group: Definition GU2022.0

Notes:

A **group** is a list of data elements. For example, a group might be a list of users, a list of commands, or a list of objects. Groups are used to facilitate the creation of queries and policy rules. Without groups, queries and policy rules might require the use of many ‘OR’ conditions. For example, when checking to see who the database user is, a query might check:

WHERE DB USER NAME = scott

OR DB USER NAME = a8000

OR DB USER NAME = a4902

OR DB USER NAME = a4949

OR DB USER NAME = a5710

OR DB USER NAME = a9449

OR DB USER NAME = sa

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

If a group named ‘-Privileged Users’ is created, and the user ids scott, a8000, a4902, a4949, a5710, a9449, and sa are added to that group, the query needs only to check:

WHERE DB USER NAME IN GROUP –Privileged Users

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Methods to build groups

There are six methods to build groups:

- Manual Entry
- Auto Generated Calling Prox
- LDAP
- Populate From Query
- Classifier
- GrdAPI

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-3. Methods to build groups GU2022.0

Notes:

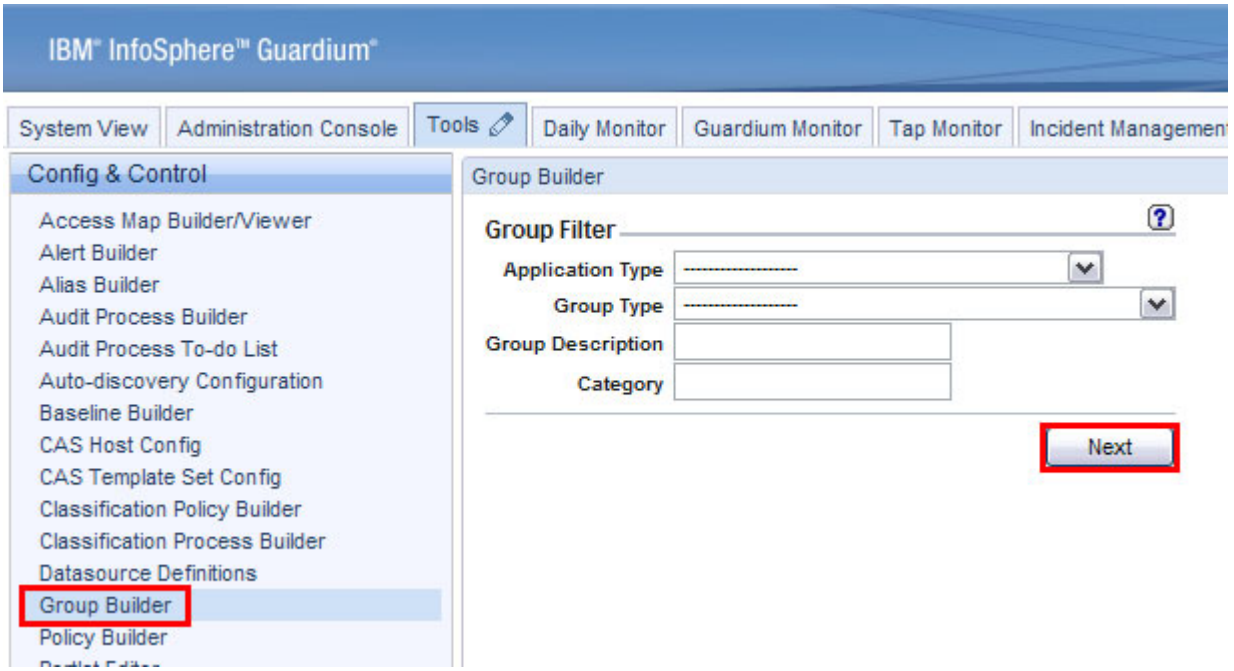
There are six different ways groups can be built and populated in Guardium. These methods include:

- Manual Entry
- Auto Generated Calling Prox
- LDAP
- Populate From Query
- Classifier
- GrdAPI

Each of these methods will be described in the upcoming pages.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Accessing Group Builder



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-4. Accessing Group Builder GU2022.0

Notes:

Groups are accessed from:

Tools > **Config & Control** > **Group Builder** as a user with the Admin role

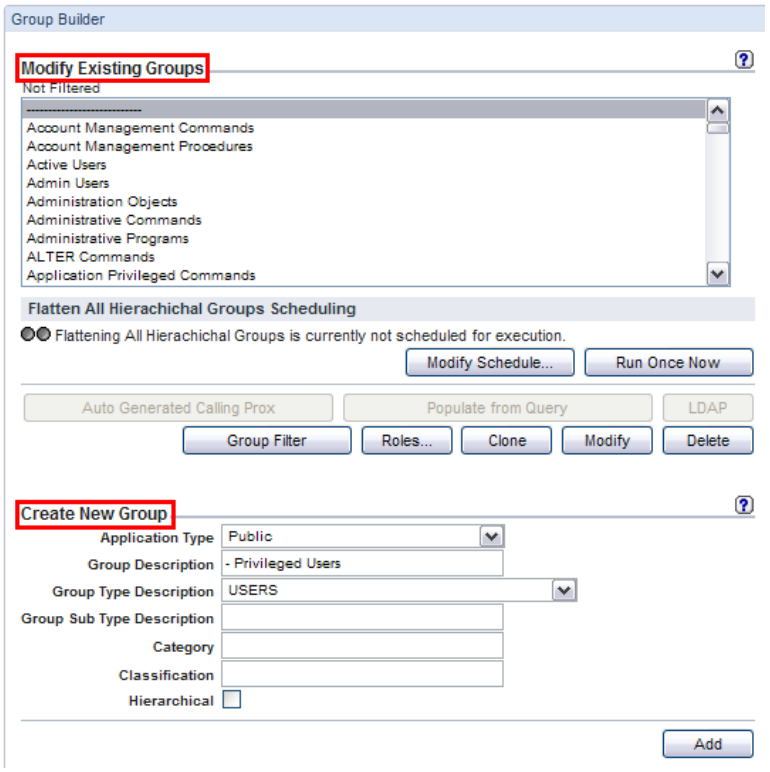
-or-

Monitor/Audit > **Build Reports** > **Group Builder** as a user with the User role

From the **Group Filter** screen, press **Next** to reach the Group Builder. Optionally, you can choose to filter the list of groups displayed in the Group Builder by choosing filter options. For example, if you only want to see user groups, you would choose *Users* under *Group Type*.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Group Builder screen overview



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-5. Group Builder screen overview GU2022.0

Notes:

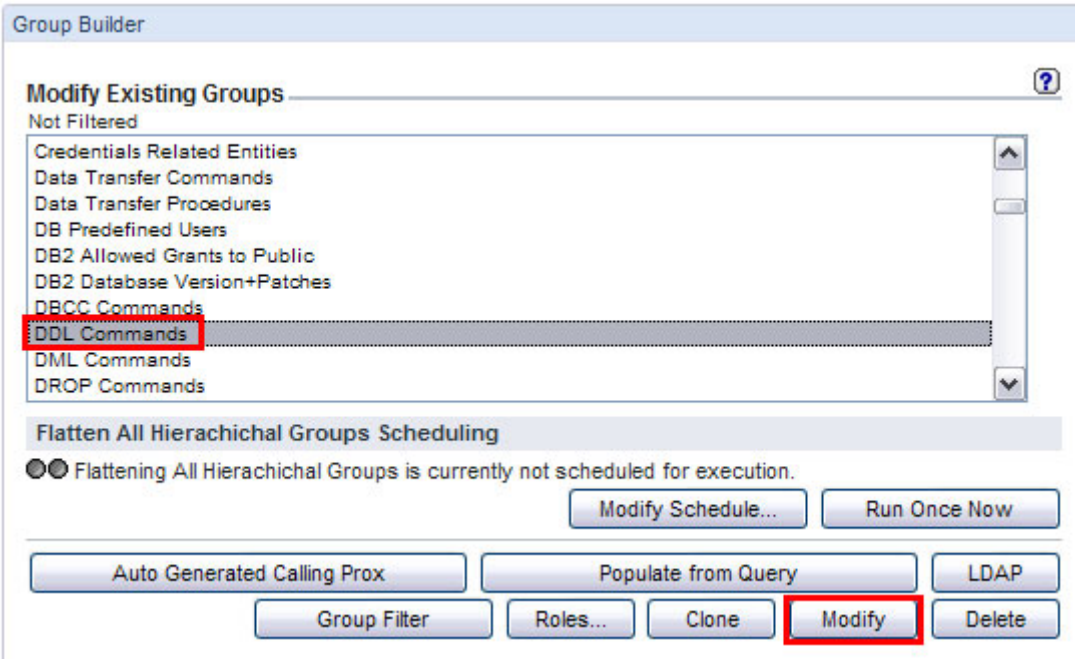
The group builder is comprised of two panes:

- Modify Existing Groups
- Create New Group

Modify Existing Groups allows you to update a preexisting group. Create New Group allows you to define a new group to Guardium.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Modify existing groups (1 of 2)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-6. Modify existing groups (1 of 2) GU2022.0

Notes:

There are a large number of built-in groups. These are provided for user convenience and are the basis for some of the built-in reports. Some groups are based on industry standards, such as the DDL and DML groups. Others are placeholders, such as the Sensitive Objects group, that allow you to enable built-in reports by simply populating the appropriate groups. In both cases, these groups can be modified.

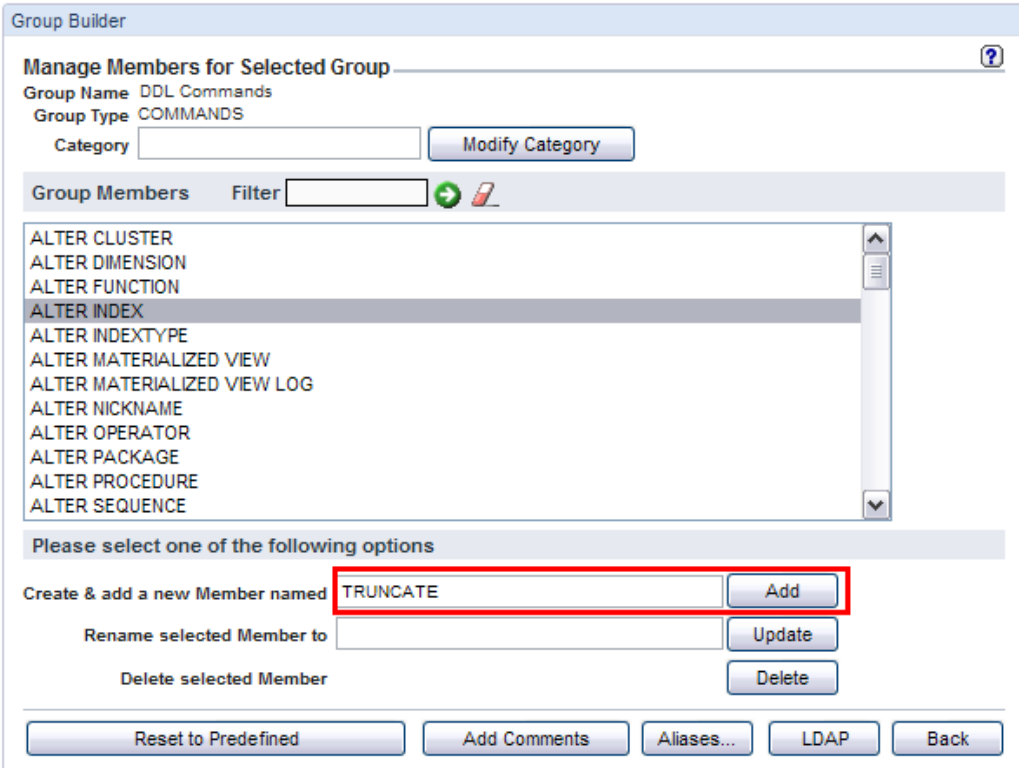
Example

Some companies consider Truncate command to be DDL, which is not included in the built-in group. To add the command to the DDL Group, highlight the group name and press the **Modify** button. (Continued on next page)

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Modify existing groups (2 of 2)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-7. Modify existing groups (2 of 2) GU2022.0

Notes:

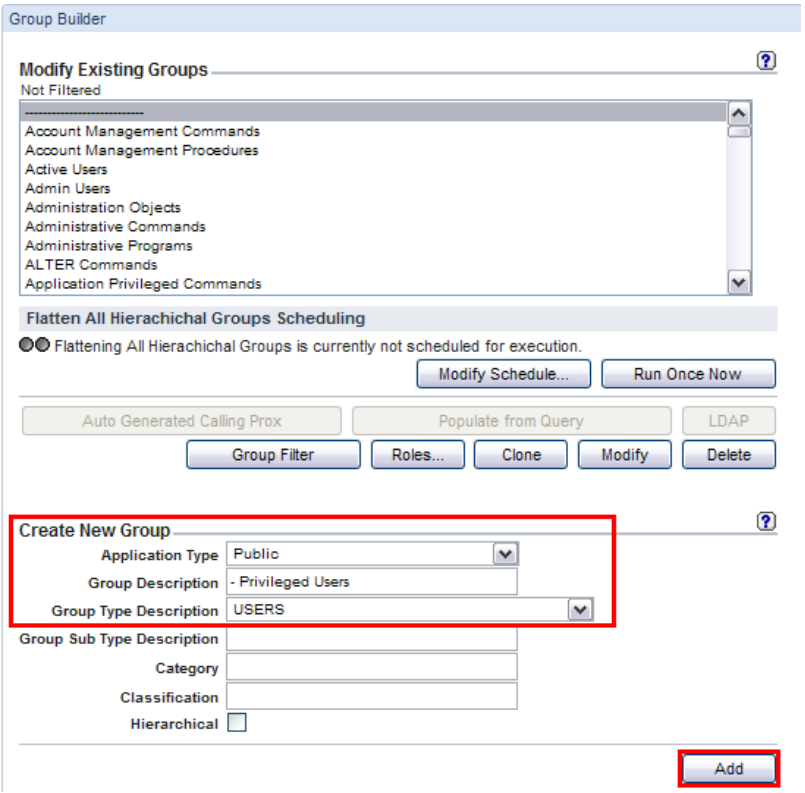
- Type in the new group member name in the **Create & add a new Member named** field and press **Add**.

Other options

- You can choose to rename existing members by highlighting the member, typing the new name in the **Rename select Member to** field, and pressing **Update**.
- To delete members highlight the member and press the **Delete** button.
- Press **Back** when complete

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Create New Group



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-8. Create New Group GU2022.0

Notes:

The following fields are required to create a new group:

- **Application Type**. This will indicate which applications will be able to access this group, with *Public* indicating all applications.
- **Group Description**. This is the name of the group. It is recommended to start the group name with a character or characters to distinguish the custom groups from the built-in groups. It this example a dash (-) is used, which also causes the group to appear at the top of the list of groups.
- **Group Type Description**. This is the data element on which you are basing your group; users, objects, client IPs, server IPs, etc.

The remaining fields are optional:

- **Group Sub Type Description**. A sub type is used to collect multiple groups of the same group type, where the membership of each group is exclusive. For example, assume that you have database servers located in three data centers, and that you

 © Copyright IBM Corp. 2011, 2013

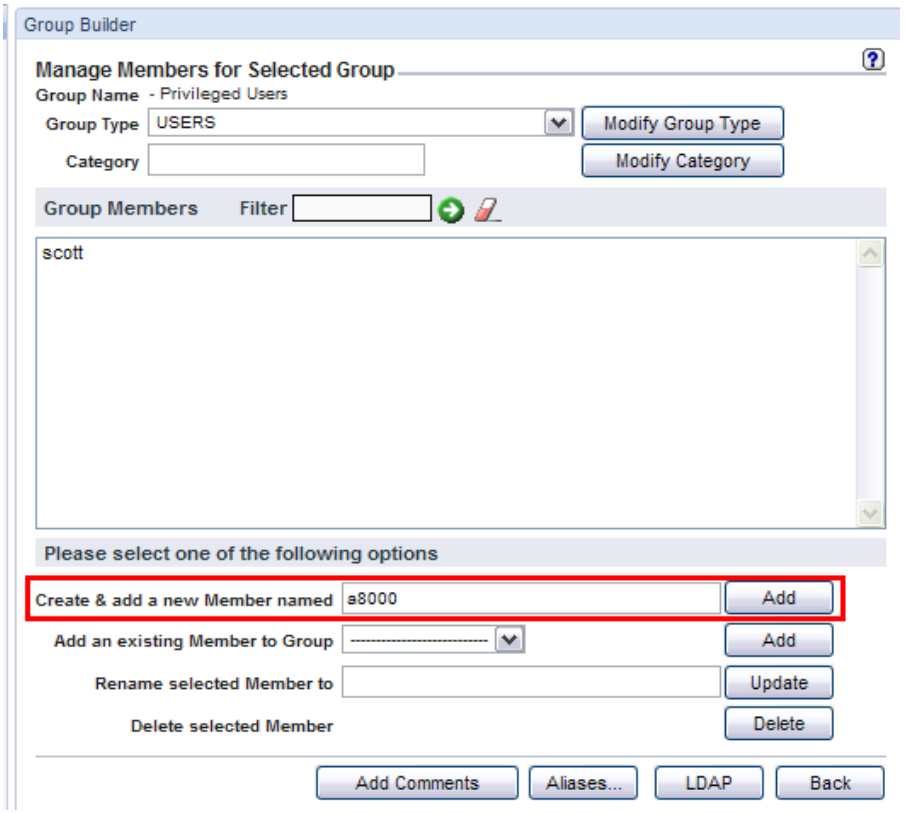
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

want to group the servers by location. You would define a separate group of database servers for each location, and define all three groups with the same sub type.

- **Category**. This is an optional label used to group items like policy violations and groups for reporting.
- **Classification.** This is another optional label used for policy violations and groups.
- **Hierarchical**: The Hierarchical check box will cause the group to be defined as a “group of groups”. This will be discussed later in this unit.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Manual entry (1 of 2)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-9. Manual entry (1 of 2) GU2022.0

Notes:

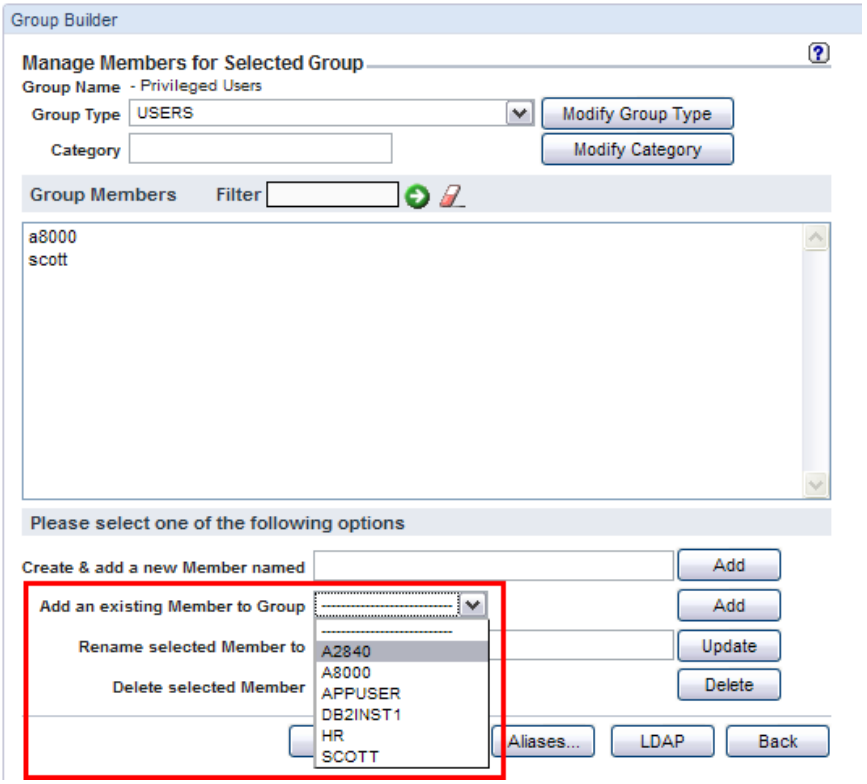
One way to add new members to a group is to manually type them in.

To add new members using this method, type the member name in the **Create & add a new Member named** field and press **Add**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Manual entry (2 of 2)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-10. Manual entry (2 of 2) GU2022.0

Notes:

Some groups will also allow you to manually choose from a pull-down list by using the **Add an existing Member to Group** field. This list is based on data logged by Guardium and will be available for groups where the size of the list will be limited. For example, the number of users logged will be in the hundreds or thousands and, thus, will have the pull down available. However, there will likely be millions of fields logged, making a pull-down list impossible.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox (1 of 2)

- Guardium operates at the network level, capturing interactive SQL requests
  - The STAP agent does not reside within the database
- For example, this DB2 ***stored procedure*** inserts values into the g_customers table:

```
CREATE PROCEDURE sp_g_customers (IN c_id_in INT,IN c_firstname_in
varchar(25),IN c_lastname_in varchar(25))
LANGUAGE SQL BEGIN
    insert into g_customers (c_id,c_firstname,c_lastname)
    values(c_id_in,c_firstname_in,c_lastname_in);
END
```

- When the stored procedure is executed, Guardium captures:

```
call sp_g_customers (?,'?','?')
```

- The individual code contained within the stored procedure is not captured when the procedure is called

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-11. Auto Generated Calling Prox (1 of 2) GU2022.0

Notes:

The second method of populating a group is called Auto Generated Calling Prox. This method of data capture allows the STAP agent to utilize minimal resources on the database server.

Guardium operates at the network level, capturing interactive SQL requests. The STAP agent does not reside in the database itself. Stored procedures are created inside the database. For example, the following SQL CREATE statement creates a DB2 stored procedure named sp_g_customers which could be used to insert values into the g_customers table.

```
CREATE PROCEDURE sp_g_customers (IN c_id_in INT,IN c_firstname_in
varchar(25),IN c_lastname_in varchar(25))
LANGUAGE SQL BEGIN
insert into g_customers (c_id,c_firstname,c_lastname)
values(c_id_in,c_firstname_in,c_lastname_in);
END
```

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

When the stored procedure is executed, all Guardium normally sees is the CALL statement, so it captures:

call sp_g_customers(?,'?','?')

The individual code contained within the stored procedure is not captured by Guardium when the procedure is called. Therefore, in this example, Guardium does not capture the insert statement that is inside the stored procedure.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox (2 of 2)

- If your monitoring is based on activity against specific tables (that is, sensitive tables), you may need to include other objects, such as views, stored procedures, synonyms, and so on, that provide alternate access to the data within the sensitive tables.
- The *Auto Generated Calling* feature facilitates the categorization of such objects.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-12. Auto Generated Calling Prox (2 of 2) GU2022.0

Notes:

Auto Generated Calling Prox allows a group to capture the internal contents of database objects such as stored procedures, synonyms, views, and so on.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox: Options

Auto Generated Calling Prox allows Guardium to:

- **Populate a Group Using Database Sources**

  All databases

- **Populate a Group Using Database Dependencies**

  Oracle and MS SQL Server Only

- **Populate a Group using Reverse Dependencies and Generate Selected Object**

  Oracle only

- **Populate a Group Using Observed Procedures**

  All databases

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-13. Auto Generated Calling Prox: Options GU2022.0

Notes:

Auto Generated Calling Prox has several options. Not all of the options are available with every database type. The four options are:

- Populate a Group Using Database Sources

  Guardium will analyze the stored procedure source code on one or more database servers.

- Populate a Group Using Database Dependencies

  Guardium will populate groups based on Database Dependencies such as Functions, Java classes, Packages, Procedures, Synonyms, Tables, Triggers and/or Views (Oracle and MS SQL Server only).

- Populate a Group Using Reverse Dependencies And Generate Selected Object

  These options from the Group auto-populate menu compute a set of objects used when starting from a set of objects. For example, starting from a set of

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

stored procedures, compute all the tables that these procedures use (Oracle only).

- Populate a Group Using Observed Procedures

Guardium will populate the group by inspecting all changes or additions to stored procedures. This keeps the mapping information up-to-date through continuous analysis of changes to stored procedures. Therefore, this function can be used to augment the *Database Sources* option described above.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox: Using DB sources

- Source Group: This group will contain objects or commands in which you are interested:
  - For example, you might be interested in stored procedures that access a group of sensitive tables.
  - A group of objects should be created that contain these sensitive tables which will serve as your **source group**.
- The Auto Generated Calling Prox will create a new object group (or append to an existing object group) that will contain all the stored procedures that access these tables.
  - This will be the **target**
- (Continued on next page)

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-14. Auto Generated Calling Prox: Using DB sources GU2022.0

Notes:

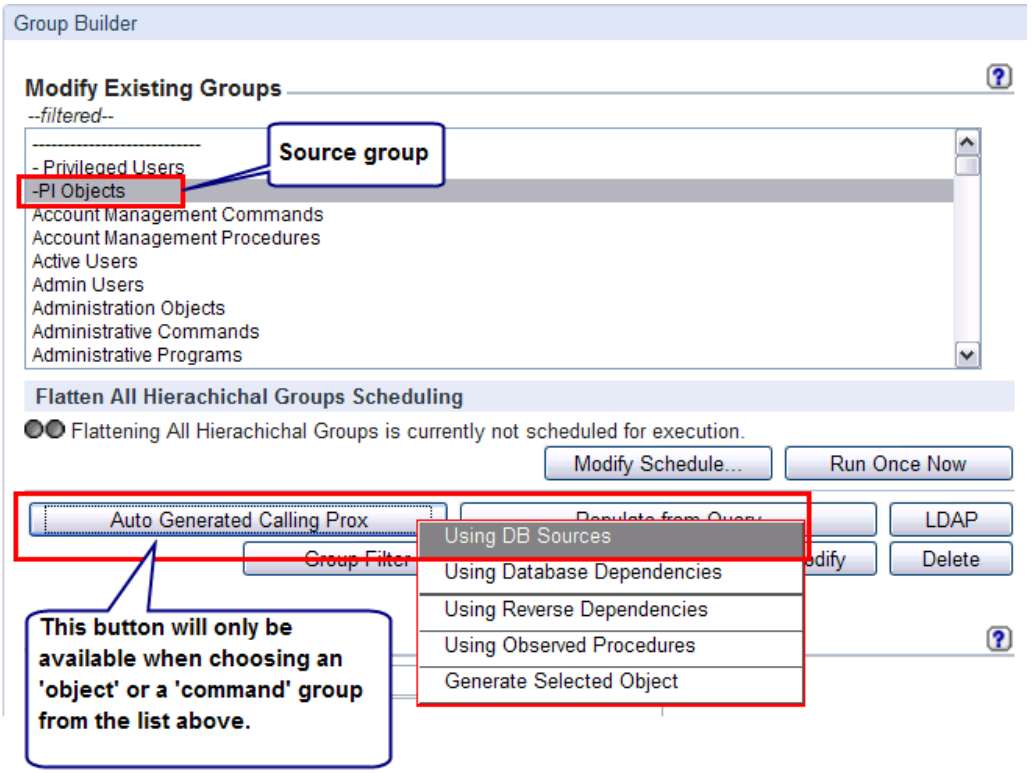
We'll now examine the Using DB Sources option within Auto Generated Calling Prox. Refer to the online Help Guide for details of the other options that were listed on the previous page.

To begin the process, you must have a *source* group. This group will contain objects or commands in which you are interested. For example, you might be interested in stored procedures that access a group of sensitive tables. A group of objects should be created that contain these sensitive tables which will serve as your **source group**.

The Auto Generated Calling Prox will create a new object group (or append to an existing object group) that will contain all the stored procedures that access these tables. This will be the **target.**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (1 of 6)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-15. Auto Generated Calling Prox example (1 of 6) GU2022.0

Notes:

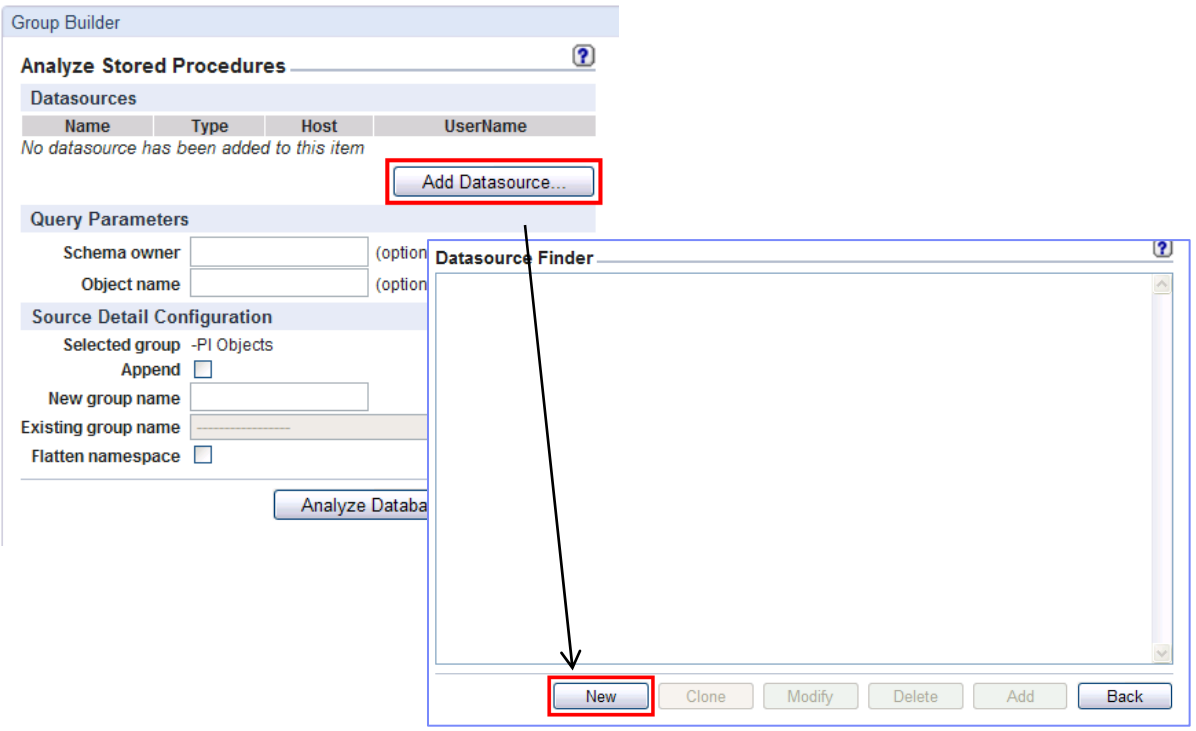
To use Auto Generated Calling Prox (using DB Sources)

- Highlight an existing *object* or *command* group.
- Press **Auto Generated Calling Prox** and choose **Using DB Sources**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (2 of 6)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-16. Auto Generated Calling Prox example (2 of 6) GU2022.0

Notes:

Next you will configure a datasource to allow Guardium to login to the database to analyze the store procedures.

- On the **Analyze Stored Procedures** screen press **Add Datasource**.
- Press **New** on the Datasource finder screen.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (3 of 6)

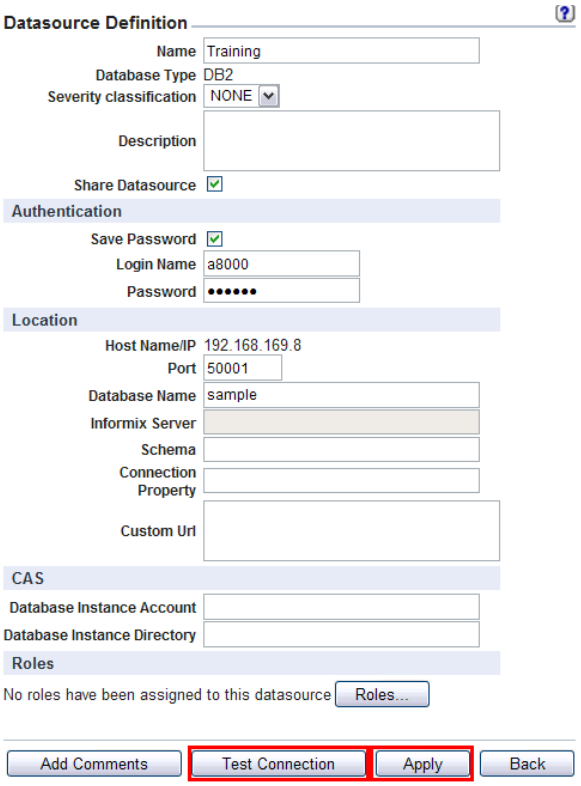


Figure 8-17. Auto Generated Calling Prox example (3 of 6) GU2022.0

Notes:

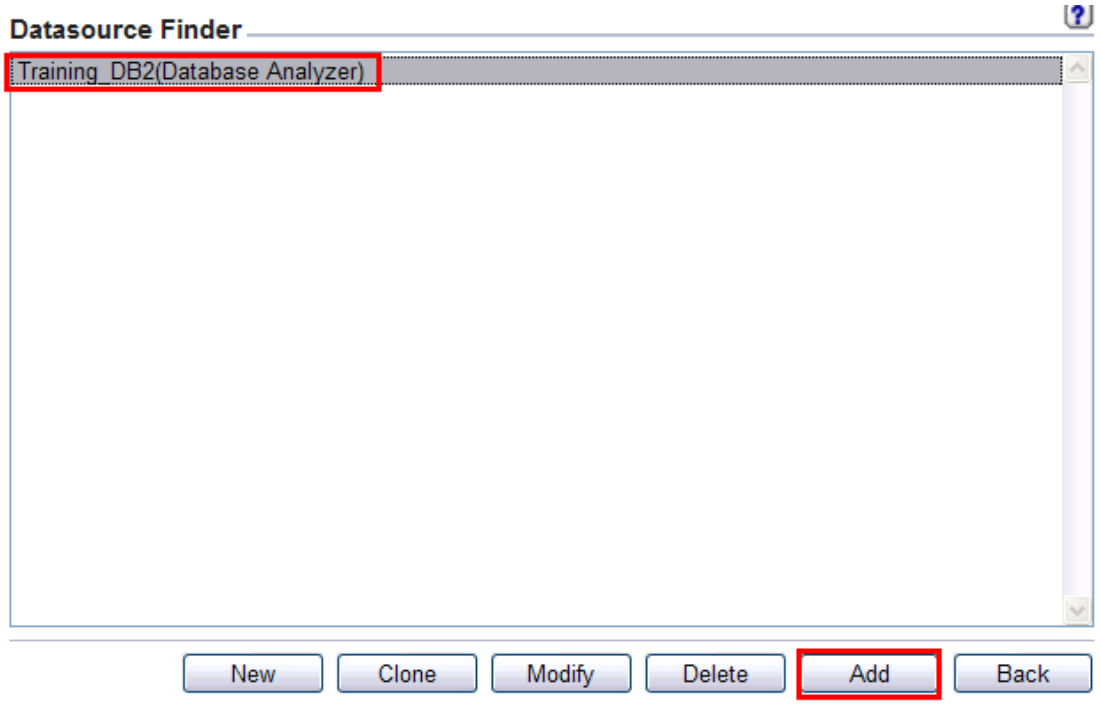
In the Datasource Definition screen:

- Enter the appropriate connection information to connect the database server
- Press **Apply** and **Test Connection**

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (4 of 6)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

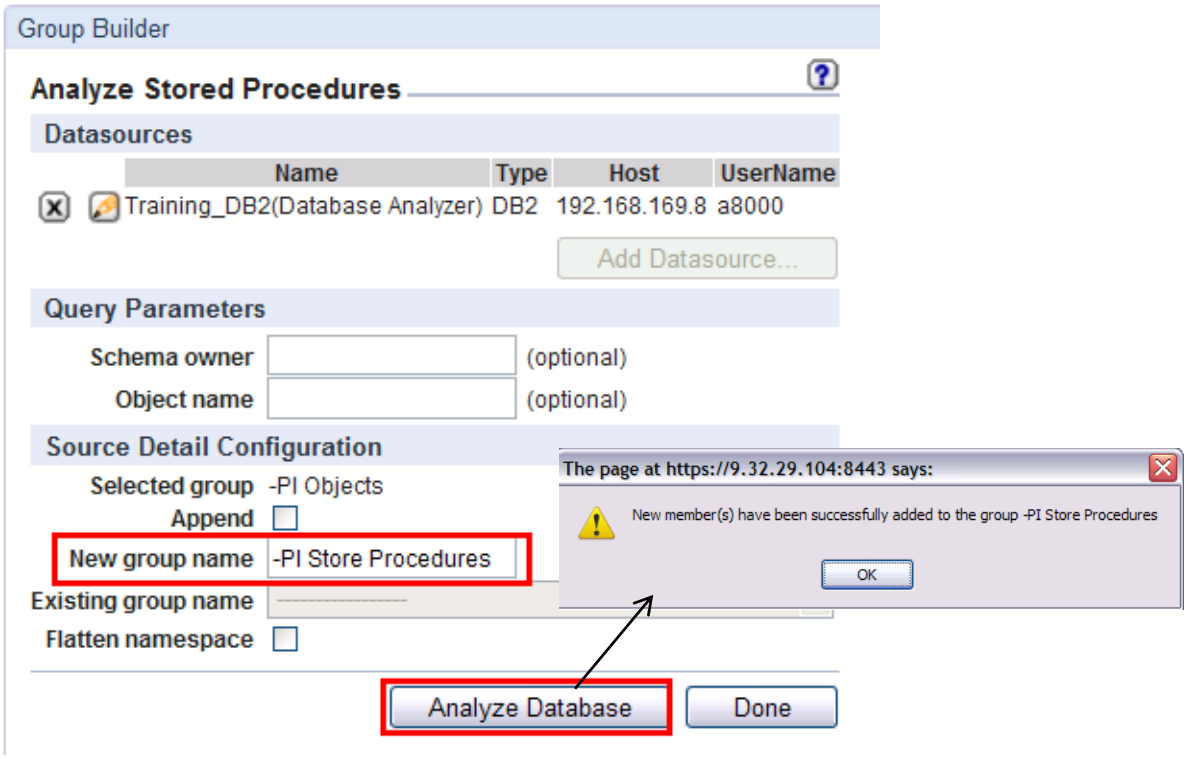
Figure 8-18. Auto Generated Calling Prox example (4 of 6) GU2022.0

Notes:

- Highlight the new datasource and press **Add**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (5 of 6)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-19. Auto Generated Calling Prox example (5 of 6) GU2022.0

Notes:

- Enter a **New group name** (or click Append and choose an Existing group name) and
- Press **Analyze Database**.

The Guardium appliance will now login to the database server and search all stored procedures for any that access any objects in the 'source group' (-PI Objects). If it finds any, you will receive a message saying that *New member(s) have been successfully added to the group –PI Stored Procedures*. The new group will be an Object group.

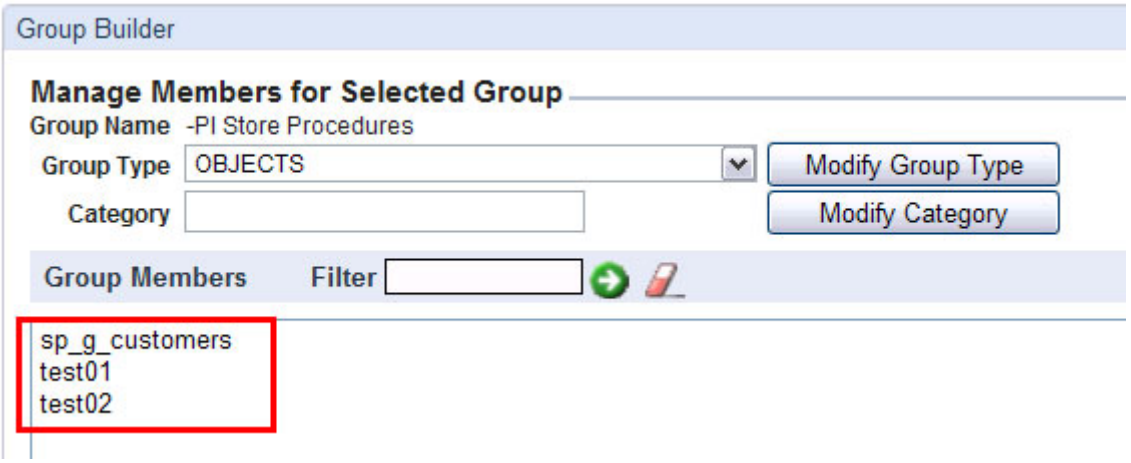
Other options

The **Flatten namespace** checkbox will apply wildcards around each of the stored procedures added to the new group.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Auto Generated Calling Prox example (6 of 6)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-20. Auto Generated Calling Prox example (6 of 6) GU2022.0

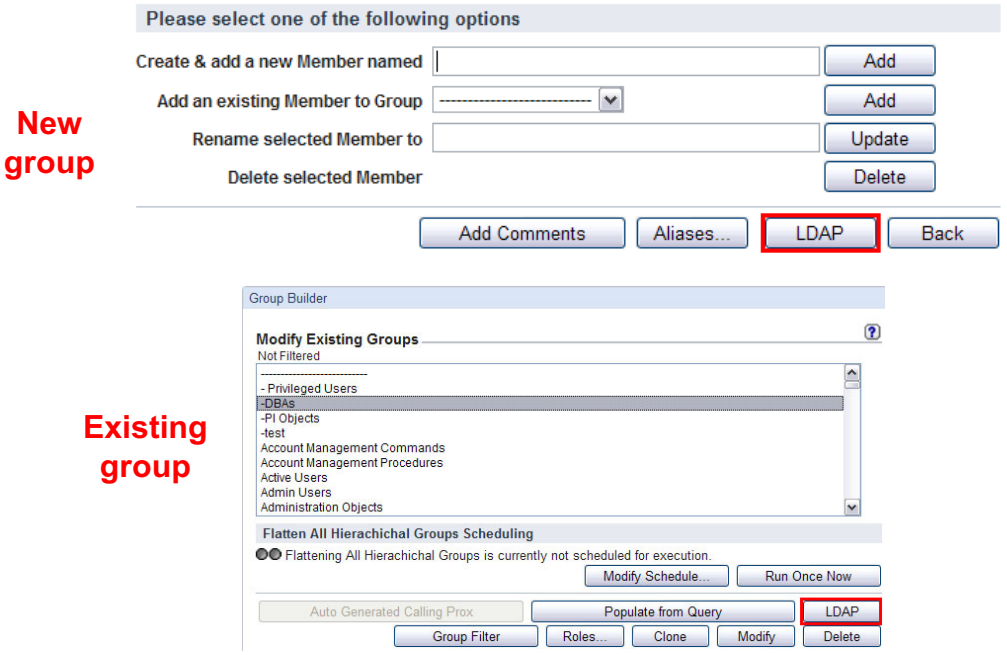
Notes:

Finally, you can view the new group to review the newly imported members.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

LDAP (1 of 2)

Groups can be populated from an LDAP sever by clicking the **LDAP** button, which is accessible when building a new group or by modifying an existing group.



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

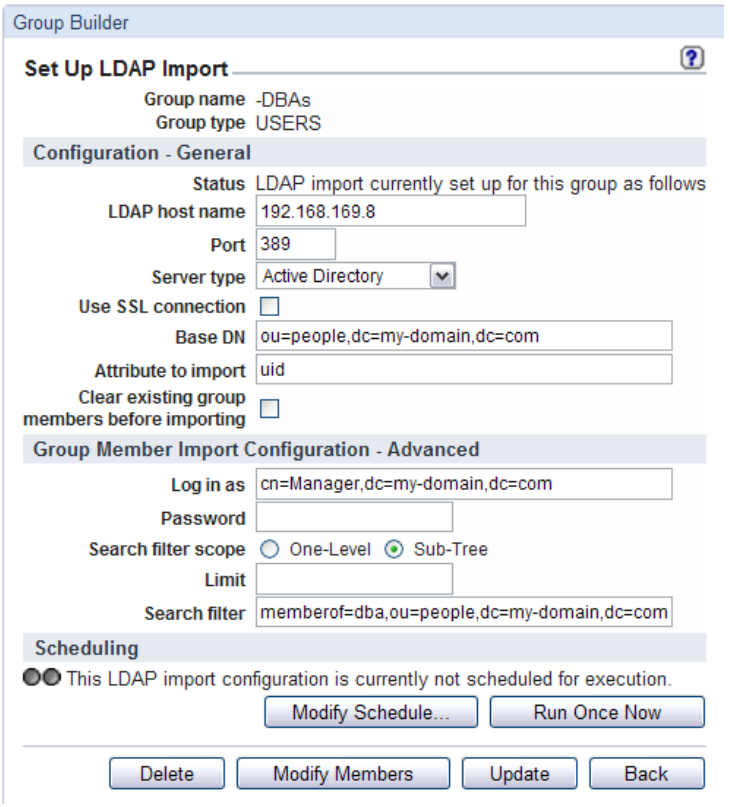
Figure 8-21. LDAP (1 of 2) GU2022.0

Notes:

A third method of populating a group is through an interaction with LDAP.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

LDAP (2 of 2)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

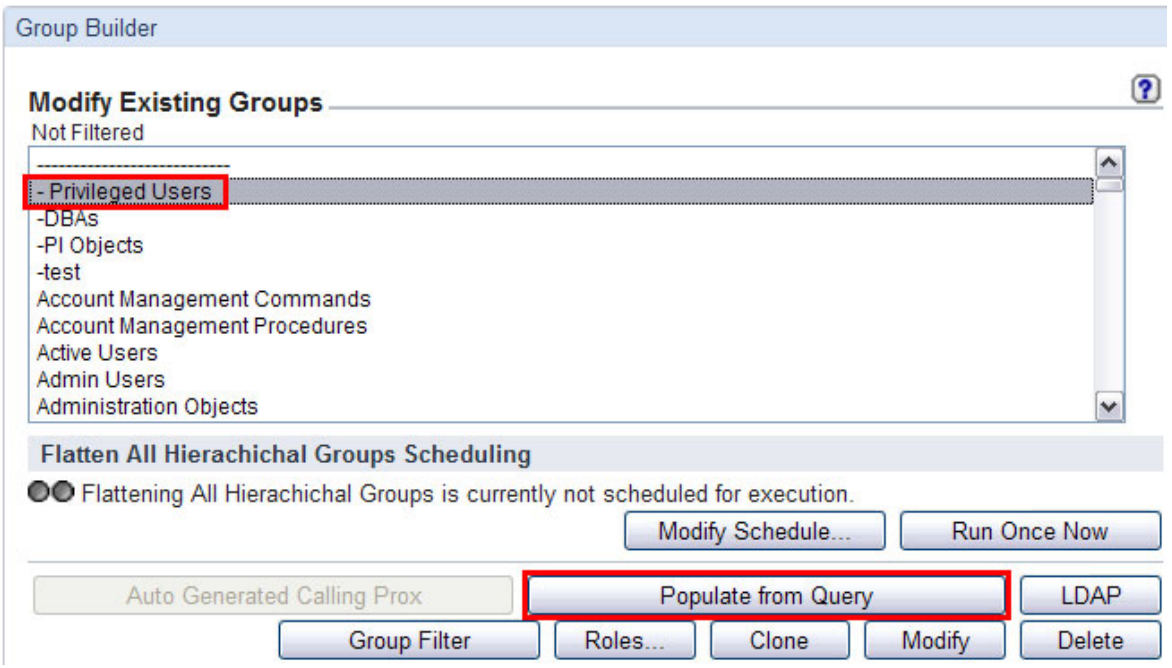
Figure 8-22. LDAP (2 of 2) GU2022.0

Notes:

- Enter the appropriate information to connect to the LDAP server.
- Press **Run Once Now**, to immediately generate a list of users to import. You can pick and choose which users you would like to import from the list.
- Or you can choose to schedule the process. If you choose the schedule the process, it will import all of the users found.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Populate from Query (1 of 4)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-23. Populate from Query (1 of 4) GU2022.0

Notes:

The fourth method of populating a group is Populate from Query.

The **Populate from Query** option allows you to add members to a group using data from Guardium's database. This data may originate from monitored database traffic or from an external source using External Data Correlation.

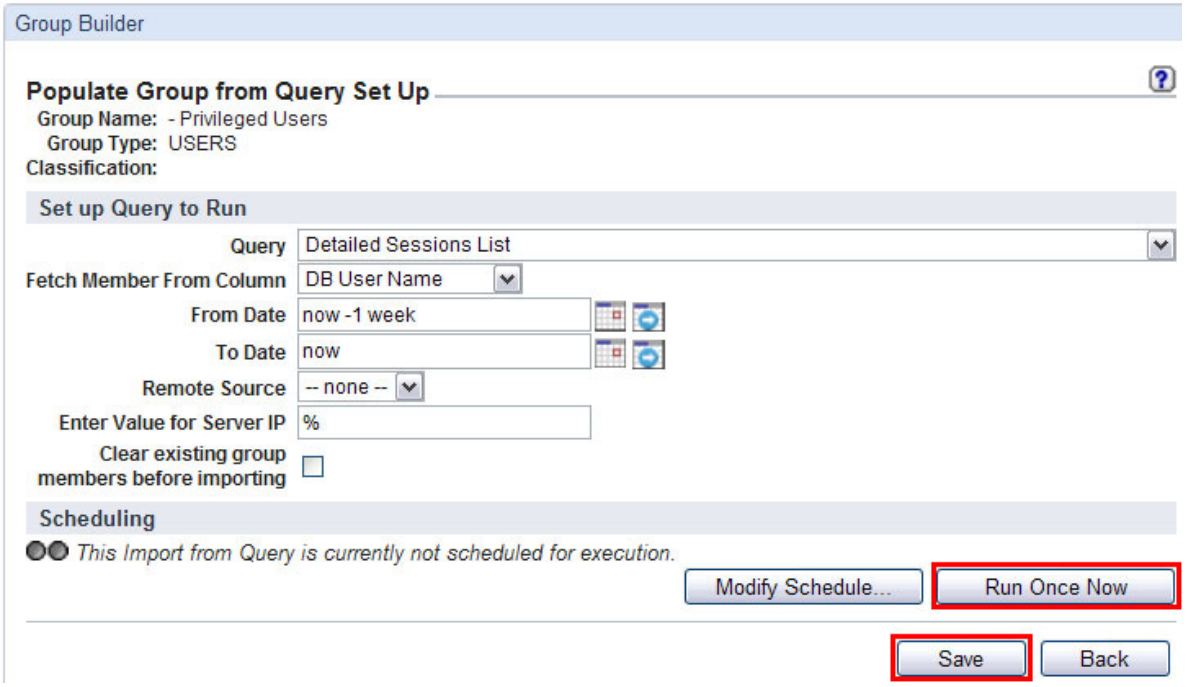
To use Populate from Query:

- Create a new group or use a previously created group
- Under **Modify Existing Groups**, highlight the group that you are interested in and press **Populate from Query**

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Populate from Query (2 of 4)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-24. Populate from Query (2 of 4) GU2022.0

Notes:

Enter the following information on the **Populate Group from Query Set Up** screen:

- **Query** – Choose the query that contains records in which you are interested. This query can be based on observed traffic or based on a customer query originating from an external source.
- **Fetch Member From Column** – Choose the field from the report that will be used to populate the group.
- **From Date** – enter the starting date and time for the query. In this example, 'now -1 week, means that the starting time of the query will be one week past from this moment.
- **To Date** – the ending point in time for this query. In the example, 'now' means the present time.
- **Remote Source** – if running this from a Central Manager, you can choose the run the query against data on a managed collector or aggregator.

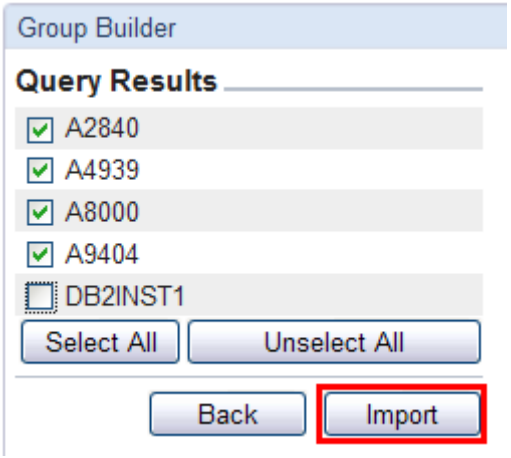
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Run time parameters** – if you have any run-time parameters enter the appropriate values or enter a percent sign (%) as a wildcard to return everything. In the example above, *Enter Value for Server IP* is a run-time parameter.
- **Clear existing group members before importing** – check this box if you want to purge all group members before importing from the query.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Populate from Query (3 of 4)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

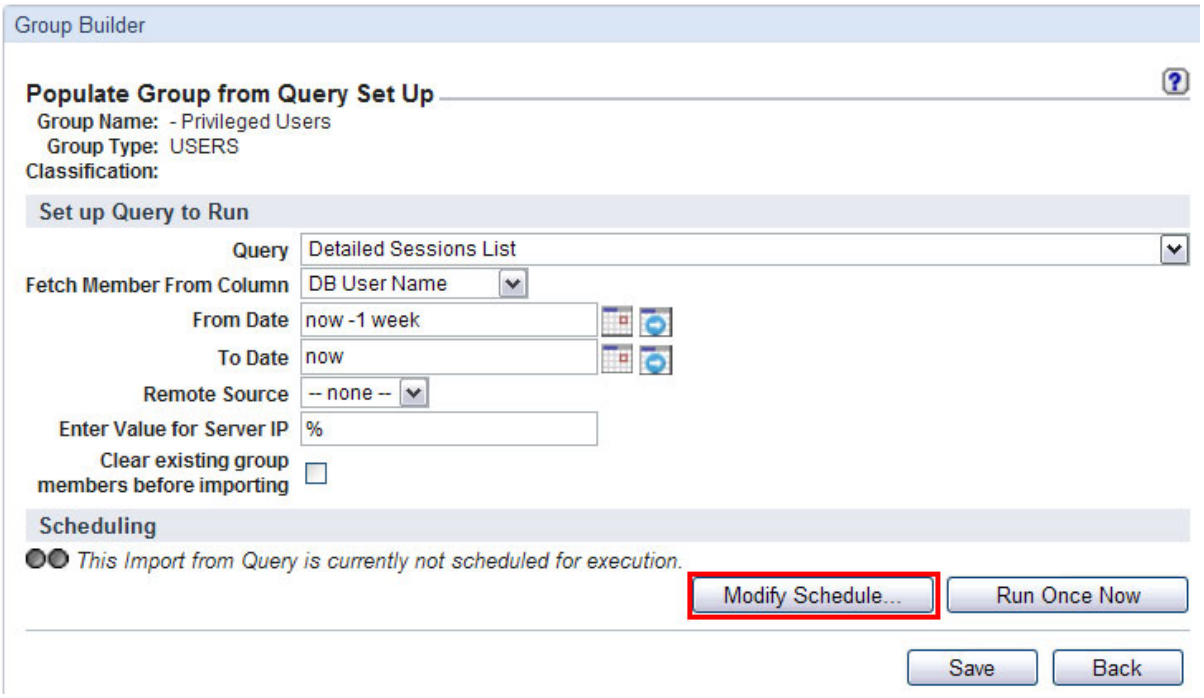
Figure 8-25. Populate from Query (3 of 4) GU2022.0

Notes:

Choose the members you would like to import and press the **Import** button.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Populate from Query (4 of 4)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-26. Populate from Query (4 of 4) GU2022.0

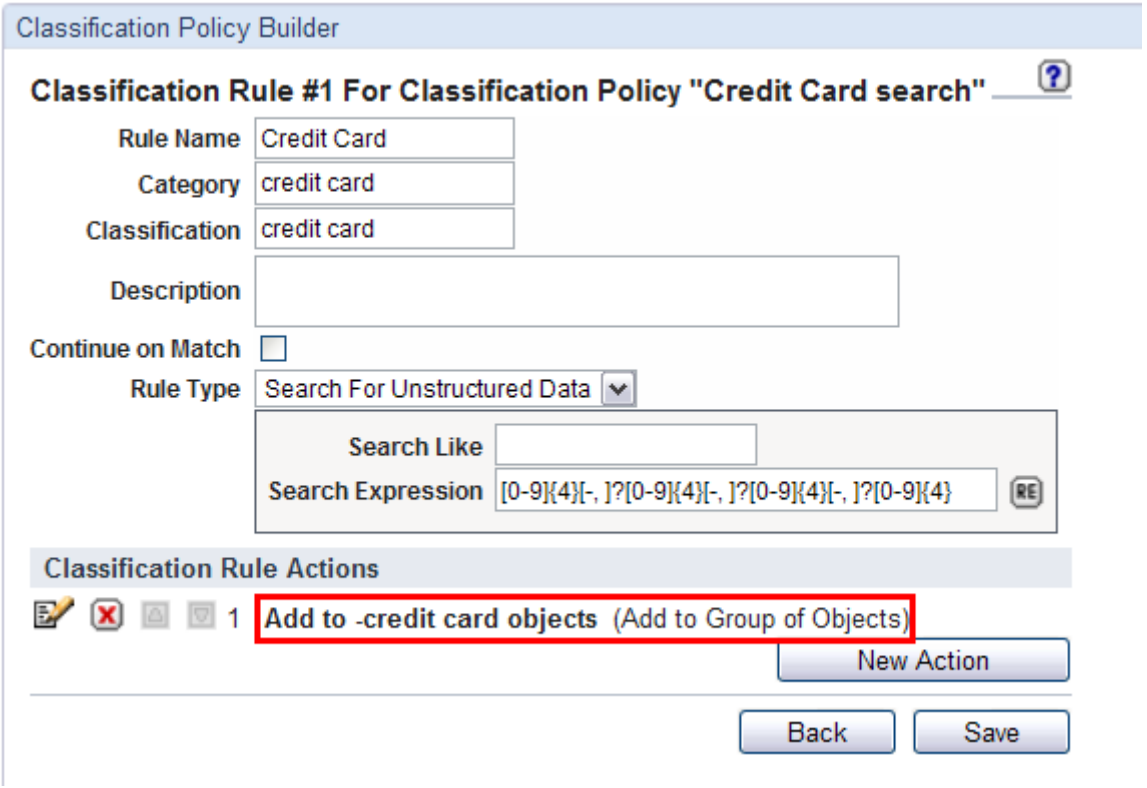
Notes:

You can also choose to import members on a scheduled basis by pressing the **Modify Schedule** button. If you choose this option, it will import all returned results. Because it is unattended, there is no option to pick specific values to import.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Classifier



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-27. Classifier GU2022.0

Notes:

The classifier will search a database and automatically add group members matching user-supplied criteria. Classification will be covered in a separate module.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GuardAPI (1 of 2)

- GuardAPI can be used to create and poplulate groups.
- You can add a member from the CLI manually:
  - grd01.guard.swg.usma.ibm.com> grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a9940
- However, it is most effective used in a batch file, as shown in the next page.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-28. GuardAPI (1 of 2) GU2022.0

Notes:

The final method of populating a group is by using GuardAPI. GuardAPI provides access to Guardium functionality from the command line or from a batch file. This allows for the automation of repetitive tasks, which is especially valuable in larger implementations.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

GuardApi (2 of 2)

- Create a file with the individual commands repeated for each group member

```
dbserver01:~ # cat group-upload.txt
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a2342
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a6732
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a4345
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a7564
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a4567
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a2233
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a5678
grdapi create_member_to_group_by_desc desc="- Privileged Users" member=a4544
```

- From a Linux or UNIX server, run the following command:
  - **ssh cli@*collector-or-central-manager-ip<file-name-created-above***
  - ***For example:***

```
dbserver01:~ # ssh cli@192.168.169.9<group-upload.txt
Pseudo-terminal will not be allocated because stdin is not a terminal.
cli@192.168.169.9's password:
Welcome cli - your last login was Tue Sep 28 08:45:29 2010
grd01.guard.swg.usma.ibm.com> ok
ID=1000008
grd01.guard.swg.usma.ibm.com> ok
ID=1000009 …
```

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

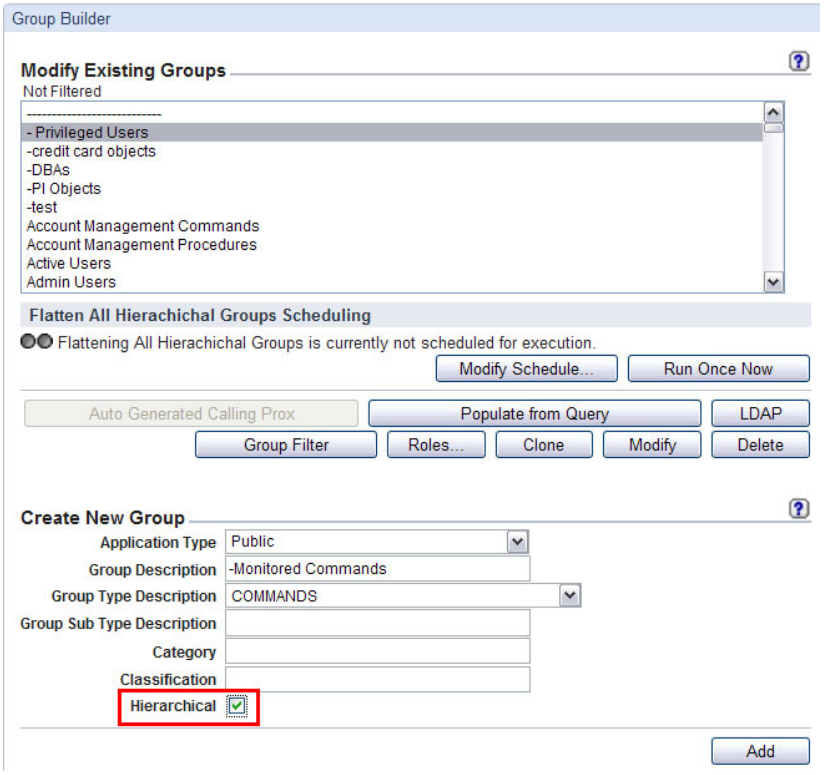
Figure 8-29. GuardApi (2 of 2) GU2022.0

Notes:

GuardAPI commands, including those to create and populate groups, can be scripted and run in batch files.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Hierarchical groups (1 of 3)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-30. Hierarchical groups (1 of 3) GU2022.0

Notes:

The **Hierarchical** checkbox allows a group to be defined as a “group of groups”. For example, if you have three groups of users (DBAs, SAs, and Developers) who are also considered to be privileged users, you could create a group called ‘Privileged Users’ that would contain the members of all three groups. This allows you to be specific when necessary (all DBA activity, for instance) while allowing for fewer steps when you have broader requirements (all Privileged user activity).

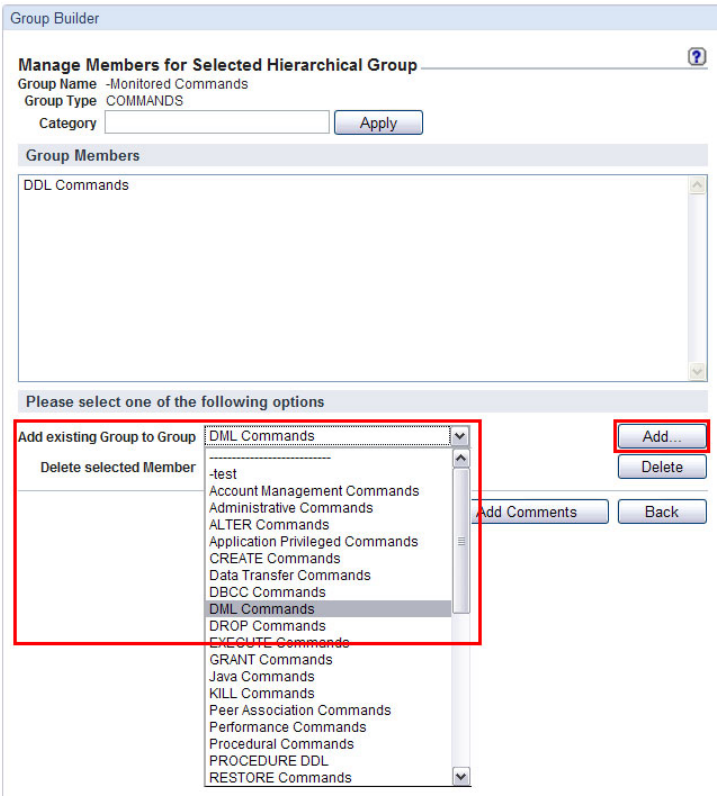
To create a Hierarchical group:

- Create a new group. In this example, we will created a group of ‘Monitored Commands’ that will contain the DML and DDL groups.
- Check the **Hierarchical** checkbox.
- Press **Add**.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Hierarchical groups (2 of 3)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-31. Hierarchical groups (2 of 3) GU2022.0

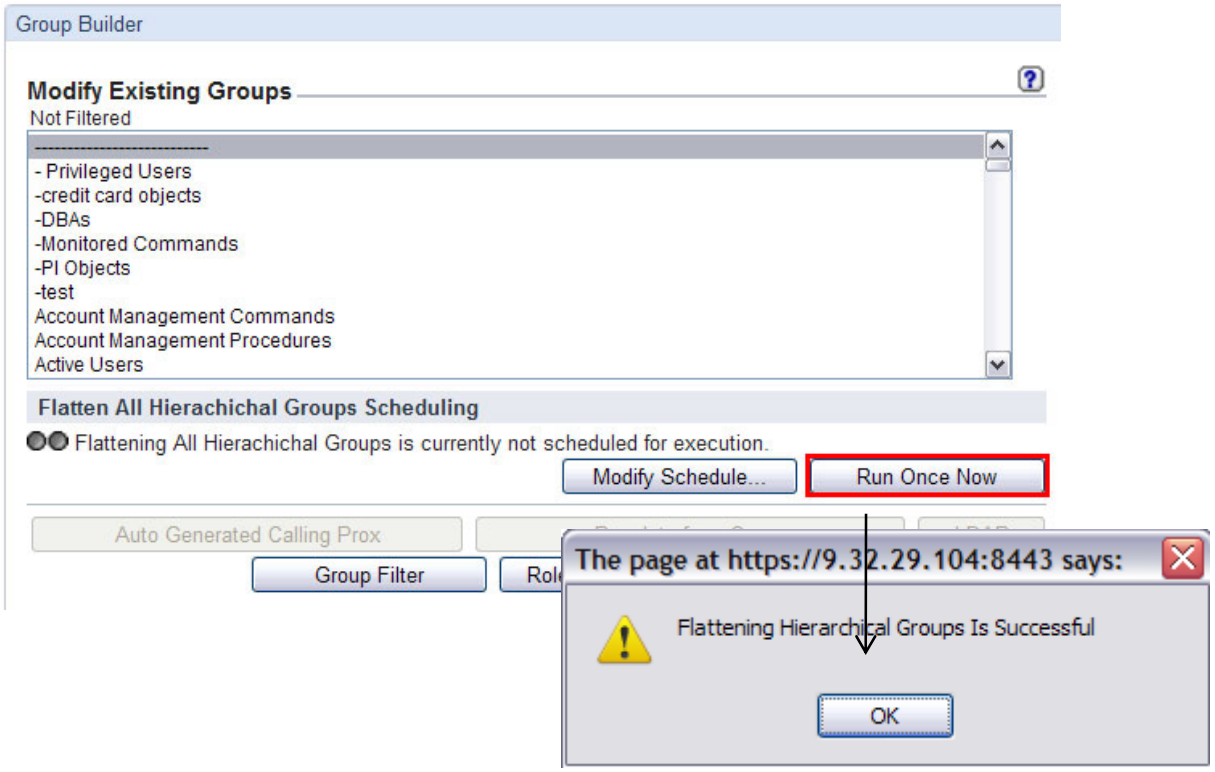
Notes:

For Hierarchical groups there is no option to type in group members. Instead, you must use the pull-down containing all of the groups matching the group type of the Hierarchical group

- From **Add existing Group to Group** choose *DDL Commands* and press **Add**.
- Repeat for *DML Commands*
- Press **Back** when you are done

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Hierarchical groups (3 of 3)



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-32. Hierarchical groups (3 of 3) GU2022.0

Notes:

To consolidate all of the sub-groups under the “group of groups” the groups must be ‘flattened’.

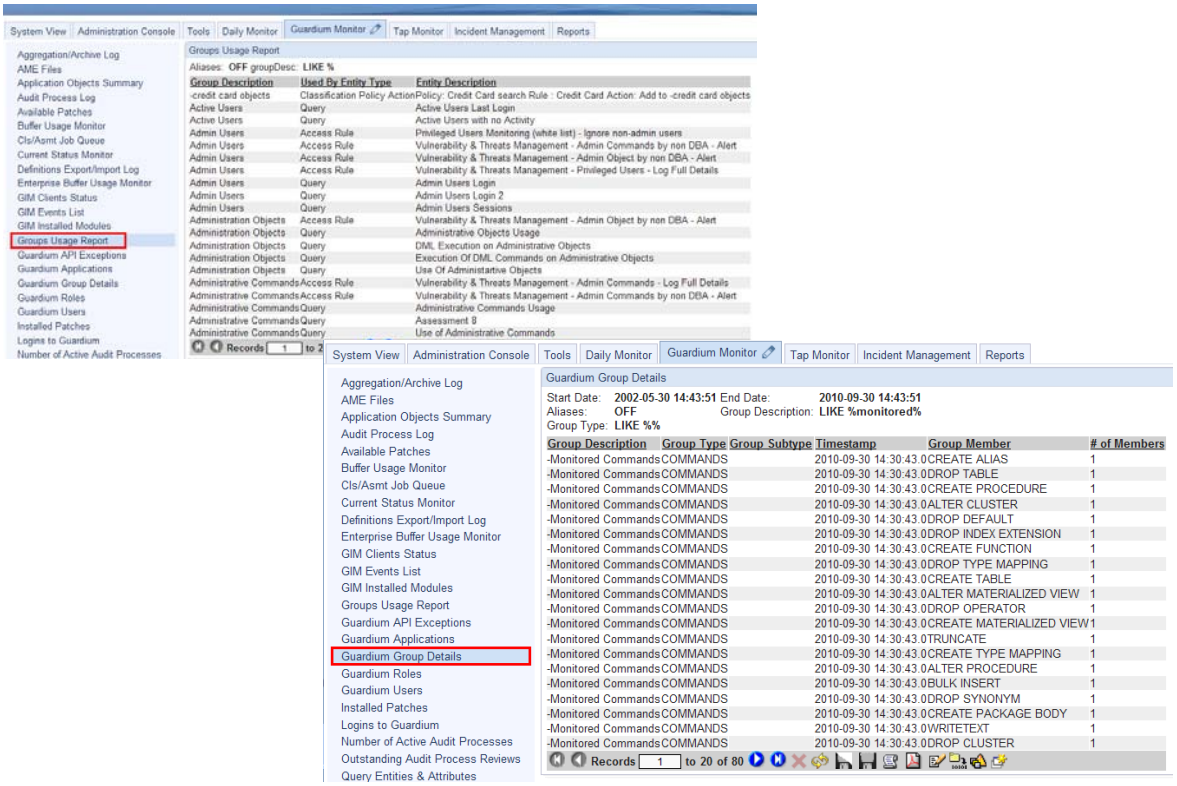
- From the **Group Builder**, press **Run Once Now** under the **Flatten All Hierarchical Groups Scheduling**
- The “group of groups” will now encompass all of the members of the ‘DDL Commands’ group and the ‘DML Commands’ group. This process should also be scheduled (by pressing the **Modify Schedule…** button), so that any changes made to either sub-group will be reflected in the hierarchical group.

To see the list of individual members in the hierarchal group, go to the **Guardium Monitor** tab and click the **Guardium Group Details** link, as shown on the next page.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Group reports



© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-33. Group reports GU2022.0

Notes:

Under **Guardium Monitor** there are two reports that provide details on all of the groups in the system:

- **Group Usage Report** – details where each group is used with the solution.
- **Guardium Group Details** – provides a list of all groups that can be filtered by description and/or group type.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. True or False? A Guardium group is always defines a group of users.
2. List the six methods used to build and populate Guardium groups.
3. Which of the following is not a built-in Guardium group?
   a. Sensitive Objects
   b. DML
   c. DDL
   d. DCL
4. True or False? Manual entry of lists always includes a drop-down list of items.
5. True or False? The Auto Generated Calling Prox option Populate a Group Using Database Sources is available on all database types.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-34. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

True or **False**? A Guardium group is always defines a group of users.

2. List the six methods used to build and populate Guardium groups.

Manual Entry

Auto Generate Calling Prox

LDAP

Populate from Query

Classifier

GuardAPI

3. Which of the following is not a built-in Guardium group?

a. Sensitive Objects

b. DML

c. DDL

d. DCL

4. True or **False**? Manual entry of lists always includes a drop-down list of items.

5. **True** or False? The Auto Generated Calling Prox option Populate a Group Using Database Sources is available on all database types.

Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (2 of 2)

6. True or False? GuardAPI can be used to script the populating of groups.
7. A(n) _____ is a “group of groups”.
8. _____ consolidates sub-groups in a hierarchy into a single group.
9. List the two types of group reports available under the Guardium Monitor tab.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-35. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

6.

7.

8.

9.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

6. **True** or False? GuardAPI can be used to script the populating of groups.
7. A **hierarchy** is a “group of groups”.
8. **Flattening** consolidates sub-groups in a hierarchy into a single group.
9. List the two types of group reports available under the Guardium Monitor tab.
    1. **Group Usage Report**
    2. **Guardium Group Details**

Additional information —

Transition statement —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand all of the options to create groups
- Create groups using the manual entry and populate from query methods

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-36. Unit summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 5** in the Exercise Guide.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-37. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (1 of 2)

1. True or **False**? A Guardium group is always defines a group of users.

2. List the six methods used to build and populate Guardium groups.
    1. **Manual Entry**
    2. **Auto Generate Calling Prox**
    3. **LDAP**
    4. **Populate from Query**
    5. **Classifier**
    6. **GuardAPI**

3. Which of the following is not a built-in Guardium group?
    a. Sensitive Objects
    b. DML
    c. DDL
    d. DCL

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-38. Checkpoint solution (1 of 2) GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (1 of 2 continued)

4. True or **False**? Manual entry of lists always includes a drop-down list of items.

5. **True** or False? The Auto Generated Calling Prox option Populate a Group Using Database Sources is available on all database types.

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-39. Checkpoint solution (1 of 2 continued) GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution (2 of 2)

6. **True** or False? GuardAPI can be used to script the populating of groups.

7. A **hierarchy** is a “group of groups”.

8. **Flattening** consolidates sub-groups in a hierarchy into a single group.

9. List the two types of group reports available under the Guardium Monitor tab.

    1. **Group Usage Report**
    2. **Guardium Group Details**

© Copyright IBM Corporation 2011, 2013© Copyright IBM Corporation 2011, 2013

Figure 8-40. Checkpoint solution (2 of 2) GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 9. Policies

Estimated time

02:30

What this unit is about

This unit describes how to define and administer policies.

What you should be able to do

After completing this unit, you should be able to:

- Understand how InfoSphere Guardium logs traffic
- Create a policy or set of policies to meet your requirements
- Install and manage policies
- Note: The following topics will not be covered during this training:
  - Baselines
  - Flat logging

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand how InfoSphere Guardium logs traffic
- Create a policy or set of policies to meet your requirements
- Install and manage policies
- Note: The following topics will not be covered during this training:
  - Baselines
  - Flat logging

© Copyright IBM Corporation 2011, 2013

Figure 9-1. Unit objectives GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

9.1. Policy overview

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Policy overview

After completing this topic, you should be able to:

- Understand the default logging behavior
- Understand the concept of *constructs*

© Copyright IBM Corporation 2011, 2013

Figure 9-2. Policy overview GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Policies defined

A policy is an ordered set of rules applied by the sniffer against each request received.

- Rule types include:
  - Access
  - Exception
  - Extrusion

© Copyright IBM Corporation 2011, 2013

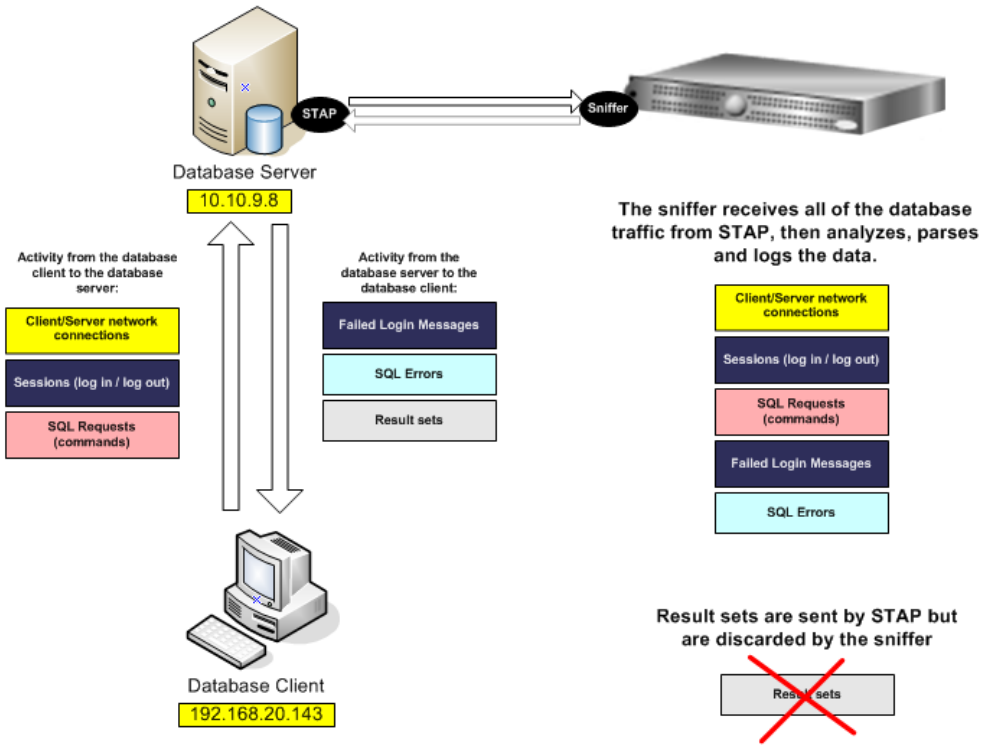
Figure 9-3. Policies defined GU2022.0

Notes:

- Each rule can apply to a request from a client or to a response from a server. Rule types include:
  - **Access** - requests from the client to the server
  - **Exception** - SQL errors and failed login messages from the server to the client
  - **Extrusion** – result sets from the server to the client
- Each rule contains conditions and one or more actions
- When all of the rule's conditions have been met the action(s) are triggered
- The rules are applied sequentially
- A policy must be installed to be in effect
  - After any change to a policy, including group member updates, the policy must be reinstalled

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Default behavior: Traffic


STAP
Sniffer
Database Server
10.10.9.8
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
Failed Login Messages
SQL Errors
Result sets
The sniffer receives all of the database traffic from STAP, then analyzes, parses and logs the data.
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Failed Login Messages
SQL Errors
Result sets are sent by STAP but are discarded by the sniffer
Result sets
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

Figure 9-4. Default behavior: Traffic GU2022.0

Notes:

To understand what a policy does, you must first understand how the system works with no policy installed – the default behavior.

Once STAP has been installed and the inspection engines configured, STAP will start forwarding all database traffic to the collector. This traffic is analyzed, parsed, and logged by the sniffer process on the collector, as follows:

Traffic sent by STAP

Database Client -> Database Server

- Client/server network connections
- Sessions (logins/logouts)
- SQL requests (commands)

Database Server-> Database Client

- Failed login messages

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- SQL errors
- Result sets

Traffic analyzed, parsed and logged by the sniffer

Database Client -> Database Server

- Client/server network connections
- Sessions (logins/logouts)
- SQL requests (commands)

Database Server-> Database Client

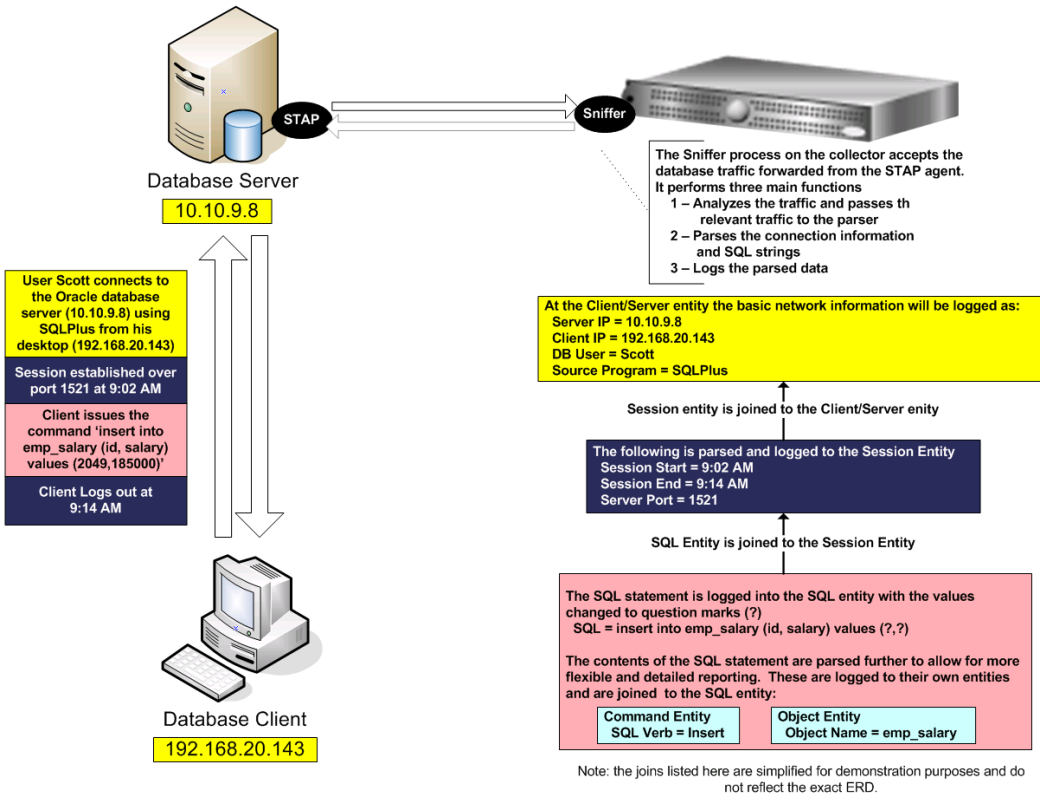
- Failed login messages
- SQL errors

Traffic ignored and discarded by the sniffer

- Result sets

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Default behavior: Parsing and logging


STAP
Sniffer
Database Server
10.10.9.8
The Sniffer process on the collector accepts the database traffic forwarded from the STAP agent.
It performs three main functions
1 – Analyzes the traffic and passes th relevant traffic to the parser
2 – Parses the connection information and SQL strings
3 – Logs the parsed data
User Scott connects to the Oracle database server (10.10.9.8) using SQLPlus from his desktop (192.168.20.143)
Session established over port 1521 at 9:02 AM
Client issues the command 'insert into emp_salary (id, salary) values (2049,185000)'
Client Logs out at 9:14 AM
At the Client/Server entity the basic network information will be logged as:
Server IP = 10.10.9.8
Client IP = 192.168.20.143
DB User = Scott
Source Program = SQLPlus
Session entity is joined to the Client/Server enity
The following is parsed and logged to the Session Entity
Session Start = 9:02 AM
Session End = 9:14 AM
Server Port = 1521
SQL Entity is joined to the Session Entity
The SQL statement is logged into the SQL entity with the values changed to question marks (?)
SQL = insert into emp_salary (id, salary) values (?,?)
The contents of the SQL statement are parsed further to allow for more flexible and detailed reporting. These are logged to their own entities and are joined to the SQL entity:
Command Entity
SQL Verb = Insert
Object Entity
Object Name = emp_salary
Database Client
192.168.20.143
Note: the joins listed here are simplified for demonstration purposes and do not reflect the exact ERD.

© Copyright IBM Corporation 2011, 2013

Figure 9-5. Default behavior: Parsing and logging GU2022.0

Notes:

When the sniffer receives the traffic from the STAP, it performs three functions against the data:

1. It **analyzes** the data to verify that it is valid SQL traffic.
2. It **parses** the data for easy reporting
   a. For example the SQL string '*insert into emp_salary (id, salary), values (2049, 185000)*' would be parsed as follows:
      i. Sentence (SQL) = insert into emp_salary (id, salary), values (?, ?)
      ii. SQL Verb = insert
      iii. Object = emp_salary
      iv. Fields = id, salary
      v. Values = 2049, 185000 (not logged by default)
3. It **logs** the parsed data into Guardium's internal database.

 © Copyright IBM Corp. 2011, 2013

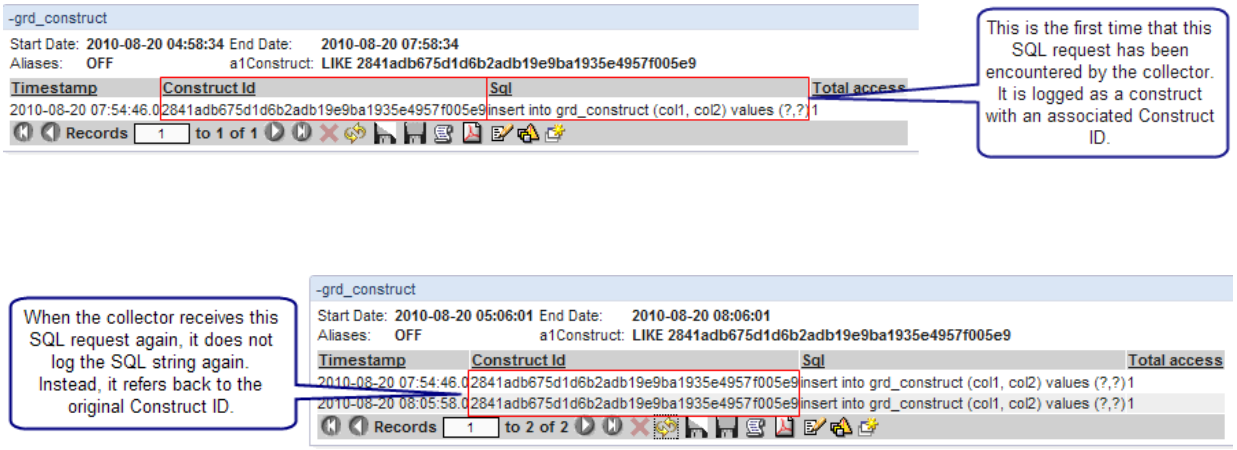
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The sniffer logs the sentence with question marks instead of the actual values entered by the user. This is done for two reasons:

1. These values can be highly sensitive and Guardium should not log this information automatically and risk exposing it to unauthorized users.
2. Masking the values allows Guardium to greatly increase the data retention on the collectors and aggregators. The next few slides will explain the concept of constructs and how masking values increases data retention.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Constructs (1 of 2)


-grd_construct
Start Date: 2010-08-20 04:58:34 End Date: 2010-08-20 07:58:34
Aliases: OFF a1Construct: LIKE 2841adb675d1d6b2adb19e9ba1935e4957f005e9
Timestamp
Construct Id
Sql
Total access
2010-08-20 07:54:46.0
2841adb675d1d6b2adb19e9ba1935e4957f005e9
insert into grd_construct (col1, col2) values (?,?)
1
Records 1 to 1 of 1
This is the first time that this SQL request has been encountered by the collector. It is logged as a construct with an associated Construct ID.
When the collector receives this SQL request again, it does not log the SQL string again. Instead, it refers back to the original Construct ID.
-grd_construct
Start Date: 2010-08-20 05:06:01 End Date: 2010-08-20 08:06:01
Aliases: OFF a1Construct: LIKE 2841adb675d1d6b2adb19e9ba1935e4957f005e9
Timestamp
Construct Id
Sql
Total access
2010-08-20 07:54:46.0
2841adb675d1d6b2adb19e9ba1935e4957f005e9
insert into grd_construct (col1, col2) values (?,?)
1
2010-08-20 08:05:58.0
2841adb675d1d6b2adb19e9ba1935e4957f005e9
insert into grd_construct (col1, col2) values (?,?)
1
Records 1 to 2 of 2

© Copyright IBM Corporation 2011, 2013

Figure 9-6. Constructs (1 of 2) GU2022.0

Notes:

When the sniffer encounters a SQL request that it has not previously seen, it logs the request as a construct with an associated primary key. Constructs are basically prototypes of requests that Guardium detects in the traffic. The combinations of commands, objects and fields included in a construct can be very complex, but each construct basically represents a very specific type of access request.

Constructs are logged with the values replaced by question marks which makes most SQL requests less unique. For example, the following statements appear to be unique to each other:

select * from employee_table where employee_id = 48 and hire_date = ‘8/2/09’

select * from employee_table where employee_id = 4940 and hire_date = ’10/29/01’

However, if you replace the values with questions marks, you will see that they are the same basic request:

select * from employee_table where employee_id = ? and hire_date = ?

select * from employee_table where employee_id = ? and hire_date = ?

 © Copyright IBM Corp. 2011, 2013

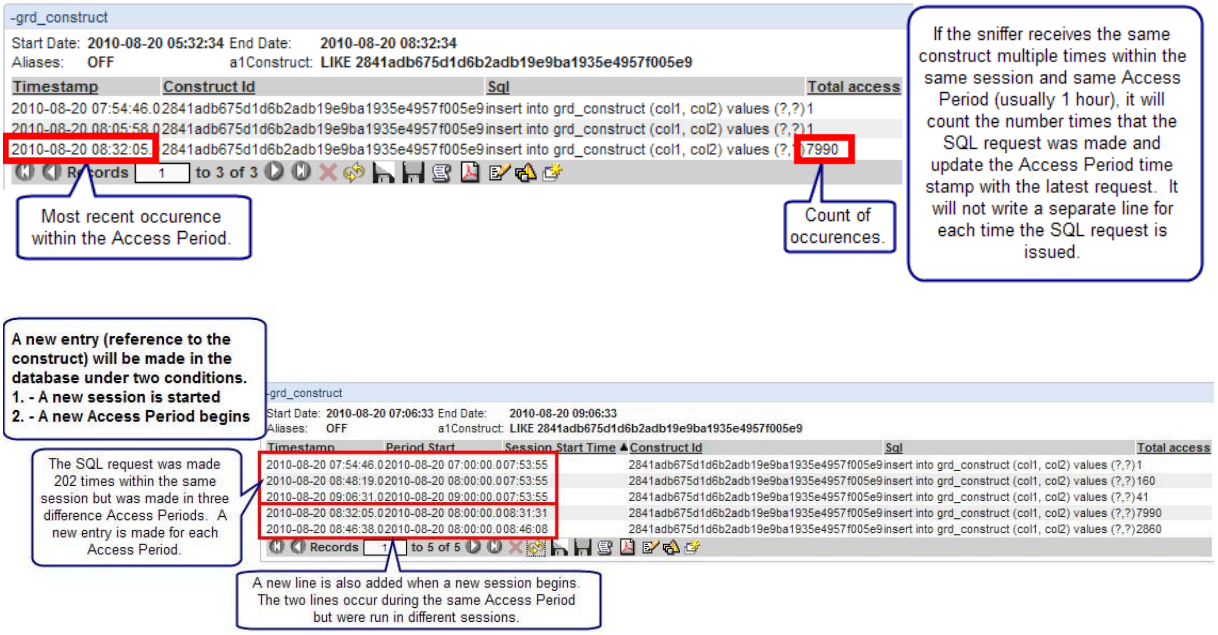
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The string, ‘select * from employee_table where employee_id = ? and hire_date = ?’, is an example of a construct. When the sniffer first encounters this SQL request it will log it with an associated construct ID. When the sniffer encounters it again, it will not log it a second time. Instead, it will refer back to construct it had logged earlier.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Constructs (2 of 2)

The default method of logging saves a tremendous amount of disk space. In the example below, the sniffer logged three entries. If each occurrence was separately logged, 7992 lines would be logged.


-grd_construct
Start Date: 2010-08-20 05:32:34 End Date: 2010-08-20 08:32:34
Aliases: OFF a1Construct: LIKE 2841adb675d1d6b2adb19e9ba1935e4957f005e9
Timestamp
Construct Id
Sql
Total access
2010-08-20 07:54:46.0 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 1
2010-08-20 08:05:58.0 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 1
2010-08-20 08:32:05. 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 7990
to 3 of 3
Most recent occurence within the Access Period.
Count of occurences.
If the sniffer receives the same construct multiple times within the same session and same Access Period (usually 1 hour), it will count the number times that the SQL request was made and update the Access Period time stamp with the latest request. It will not write a separate line for each time the SQL request is issued.
A new entry (reference to the construct) will be made in the database under two conditions.
1. - A new session is started
2. - A new Access Period begins
-grd_construct
Start Date: 2010-08-20 07:06:33 End Date: 2010-08-20 09:06:33
Aliases: OFF a1Construct: LIKE 2841adb675d1d6b2adb19e9ba1935e4957f005e9
Timestamp
Period Start
Session Start Time
Construct Id
Sql
Total access
2010-08-20 07:54:46.0 2010-08-20 07:00:00.0 07:53:55 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 1
2010-08-20 08:48:19.0 2010-08-20 08:00:00.0 07:53:55 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 160
2010-08-20 09:06:31.0 2010-08-20 09:00:00.0 07:53:55 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 41
2010-08-20 08:32:05.0 2010-08-20 08:00:00.0 08:31:31 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 7990
2010-08-20 08:46:38.0 2010-08-20 08:00:00.0 08:46:08 2841adb675d1d6b2adb19e9ba1935e4957f005e9 insert into grd_construct (col1, col2) values (?,?) 2860
Records 1 to 5 of 5
The SQL request was made 202 times within the same session but was made in three difference Access Periods. A new entry is made for each Access Period.
A new line is also added when a new session begins. The two lines occur during the same Access Period but were run in different sessions.

© Copyright IBM Corporation 2011, 2013

Figure 9-7. Constructs (2 of 2) GU2022.0

Notes:

If the sniffer receives the same construct multiple times within the defined Access Period (usually one hour) and within the same session, it counts the number of times it receives the construct and updates the Access Period Timestamp to the time of the last request. So, in reporting the finest level of detail you will see is that the construct was run *x* number of times within an hour with a timestamp representing the latest occurrence.

When the sniffer receives the same construct multiple times over an extended time period it will make new entries in the database in two cases:

1. The user starts a new session. When a new session starts, a new record is entered with its own Access Period timestamp and counter. All further occurrences of this construct within this session will update this record's Access Period timestamp and counter until a new Access Period begins as described below.
2. When a new Access Period begins within the same session. The default access period is one hour (9:00 to 9:59, 10:00 to 10:59, etc.). When a new access period begins, the next occurrence will be be entered as a new line with its own Access Period timestamp and counter.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

This method of logging saves a tremendous amount of space. As show in the examples above, thousands of requests can be collapsed into just a few lines. If each line is written separately the disk will be filled up very quickly. In a production environment, millions of lines per hour can be saved in this manner.

From an user perspective the most important things to remember about constructs are:

1. You will see a masked SQL string (question marks instead of values)
2. If the collector logs same construct within an hour from the same session
   a. It will count the number of times the construct occurred
   b. It will update the Access Period Timestamp with the time of the most recent occurrence (this will be the most precise timestamp under these circumstances)

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Checkpoint

1. A _____ is a set of rules applied by the sniffer (collector) against every request received.

2. The three types of rules are _____, _____, and _____.

3. A _____ with a primary key is created for each new SQL request that the collector encounters.

© Copyright IBM Corporation 2011, 2013

Figure 9-8. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. A **policy** is a set of rules applied by the sniffer (collector) against every request received.

2. The three types of rules are **access**, **exception**, and **extrusion**.

3. A **construct** with a primary key is created for each new SQL request that the collector encounters.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Understand the default logging behavior
- Understand the concept of *constructs*

© Copyright IBM Corporation 2011, 2013

Figure 9-9. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. A **policy** is a set of rules applied by the sniffer (collector) against every request received.

2. The three types of rules are **access**, **exception**, and **extrusion**.

3. A **construct** with a primary key is created for each new SQL request that the collector encounters.

© Copyright IBM Corporation 2011, 2013

Figure 9-10. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

9.2. Installing and creating policies

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Installing and creating policies

After completing this topic, you should be able to:

- Install a policy
- Access the policy builder
- Create a new policy

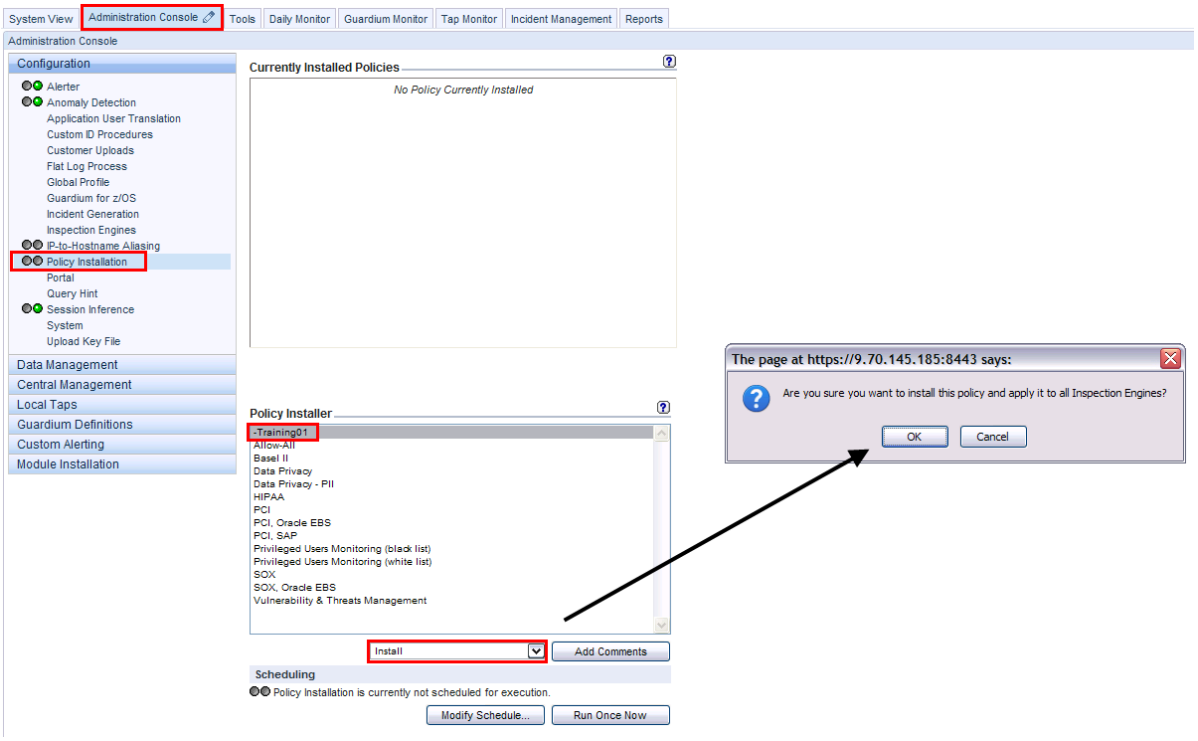
© Copyright IBM Corporation 2011, 2013

Figure 9-11. Installing and creating policies GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Install policy



© Copyright IBM Corporation 2011, 2013

Figure 9-12. Install policy GU2022.0

Notes:

The remainder of this unit will focus on creating policies and configuring policy rules. However, for a policy, or any changes to a policy, to take effect, it must be installed.

To install a policy:

- Go to the **Administration Console**, **Policy Installation**
- Highlight the policy that you would to install and choose **Install** from the drop down list

If the groups contained within the policy are updated regularly, the installation should be scheduled by clicking **Modify Schedule** to open the general-purpose scheduling utility. For example, if you are using ‘Populate from Query’ to update a group of privileged users nightly, the policy should be scheduled to be reinstalled after the group update.

More than one installed policy is permitted at the same time. All installed policies are available for action and are run sequentially. The only limitation is that policies defined as selective audit policies can not be mixed with polices not defined as selective audit policies. If trying to mix policies, an error message will result when installing these mixed policies.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

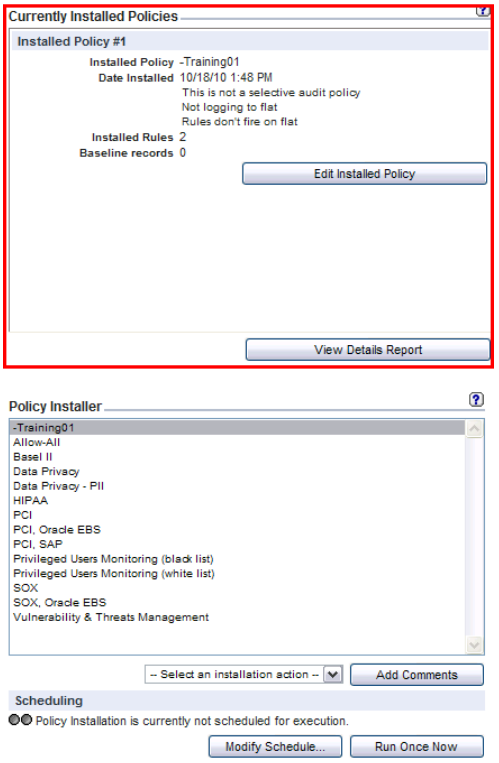
The order of appearance can be controlled during the policy installation, such as first, last or somewhere in between. But the order of appearance can not be edited at a later date.

Remember – in all of the following examples, the policy must be installed after any modifications for the changes to take effect.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Currently Installed Policies



© Copyright IBM Corporation 2011, 2013

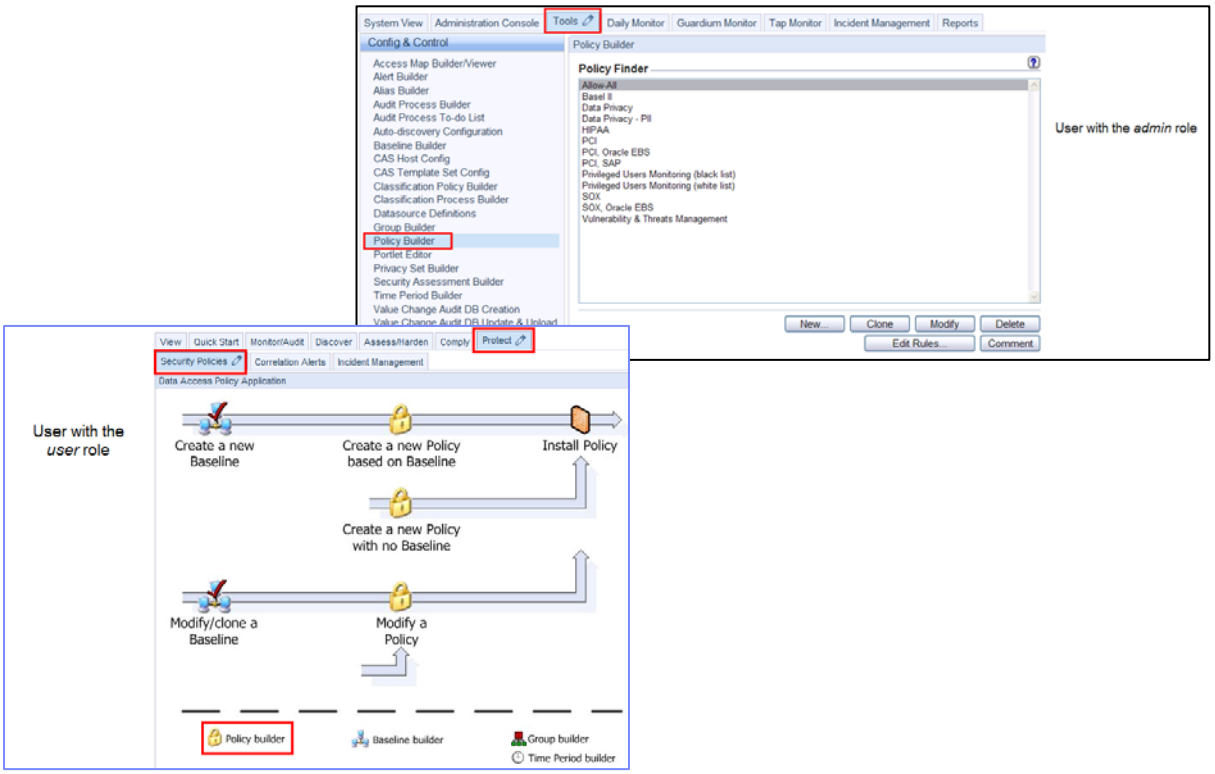
Figure 9-13. Currently Installed Policies GU2022.0

Notes:

After the policy has been installed, you can view the basic attributes (date installed, number of rules, etc) of the policy from the **Currently Installed Policies** screen. You can also directly access the policy by pressing **Edit Installed Policy**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Accessing the Policy Builder



© Copyright IBM Corporation 2011, 2013

Figure 9-14. Accessing the Policy Builder GU2022.0

Notes:

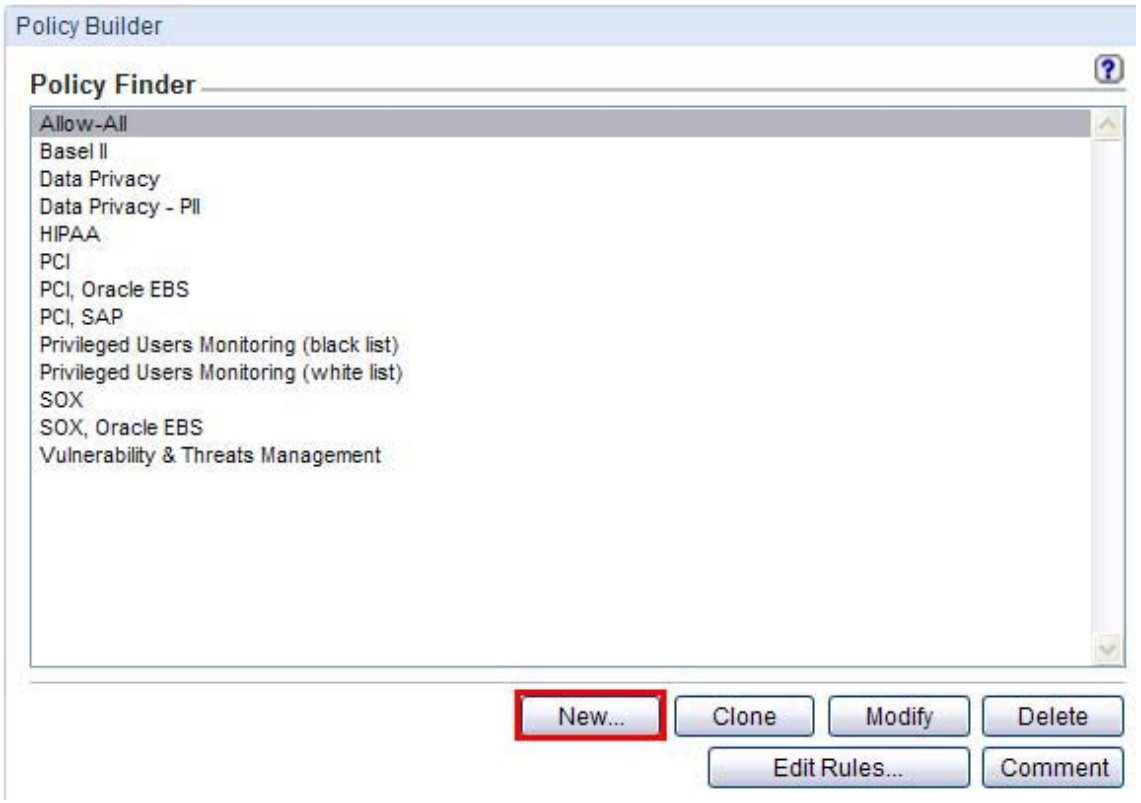
To access the Policy Builder:

- As a user with the *admin* role go to **Tools -> Policy Builder**
- As a user with the *user* role go to **Protect-> Security Policies -> Policy builder**

The remainder of the slides show how to manage policies as an *admin* user.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Create a new policy



© Copyright IBM Corporation 2011, 2013

Figure 9-15. Create a new policy GU2022.0

Notes:

Under the Policy Builder screen you will find:

- **Policy Finder**:
  - Lists the existing policies accessible by the user who is currently logged in. For access to an existing policy, you must either be the creator of the policy or belong to a role that has been granted access to it.
  - In this example, these are the policies owned by the *admin* user and are built-in to the system.
    - The **Allow-all** policy contains no rules. If you need to go back to the collector's default behavior, as described earlier in this unit, installing the *Allow-all* policy will bring you there.
    - The remaining built-in policies (*Base II*, *Data Privacy*, *Sox*, *etc.*) provide example rules to help users build their own policies. If you choose to use one of these policies in your environment, make sure that you understand what each rule does.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

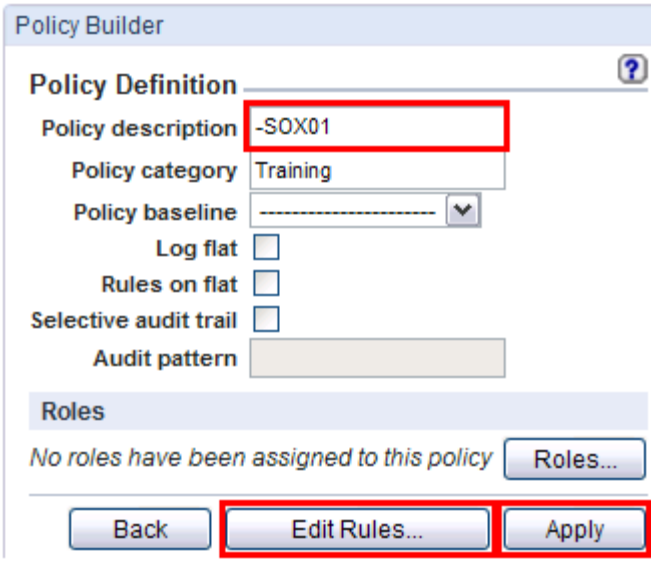
- **New…** will create a new policy
- **Clone** copies the highlighted policy, allowing you to save it with a new name
- **Modify** allows you to change the policy definition
- **Delete** removes the policy from the appliance
- **Edit Rules…** take you directly to the rules screen
- **Comment** allows you to leave notes for your self or other users

The next slides will demonstrate the steps taken after pressing the **New…** button to create a new policy.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Policy Definition (1 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 9-16. Policy Definition (1 of 2) GU2022.0

Notes:

To create a new policy, you must enter a **Policy description**. You should name the policy something that differentiates it from the built-in policies. In the example above the dash (-) helps to show that it is not a built-in policy and causes the policy to appear at the top of the list.

The remaining fields are optional:

- **Policy category** - an arbitrary label that can be used to group policy violations for reporting purposes. The category specified here will be used as the default category for each rule (and it can be overridden in the rule definition)
- **Policy baseline** - if you have created a baseline, you can create a policy based on it. This is outside the scope of this training.
- **Log flat** (not covered in this training) – This option can be used in extremely high volume environments. When this box is checked:
  - Data will not be parsed in real-time
  - The flat logs can be seen on a designated Flat Log List report

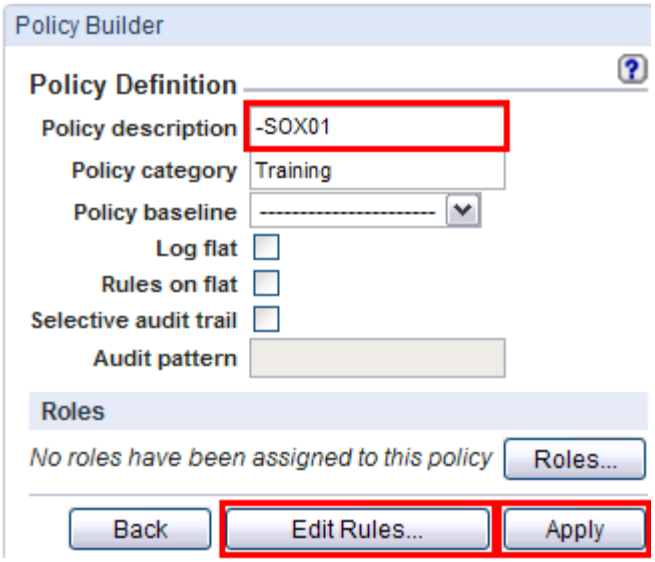
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

    - The offline process to parse the data and merge to the standard access domains can be configured through the Administration Console -> Configuration -> Flat Log Process
- **Rules on flat** (not covered in this training) – This only applicable when **Rules on flat** is checked and will result in the following behavior
    - Session-Level rules will be examined in real-time.
    - No rules will be evaluated when the offline processing does takes place.
    - When **Rules on flat** is NOT checked:
        - Policy rules will fire at processing time using the current installed policy at processing time.
- **Selective audit trail** – This will cause a special type of policy to be created that will cause all SQL requests to be dropped by the sniffer. Only SQL requests defined in the Audit Pattern or in individual rules will be logged. Failed logins, SQL errors and session-level information will be logged. Creating and installing a policy with this box checked will change the default behavior, even with no rules defined. This will be covered as a separate topic within this unit.
- **Audit pattern** - used in conjunction with the **Selective audit trail** checkbox, as described above.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Policy Definition (2 of 2)



© Copyright IBM Corporation 2011, 2013

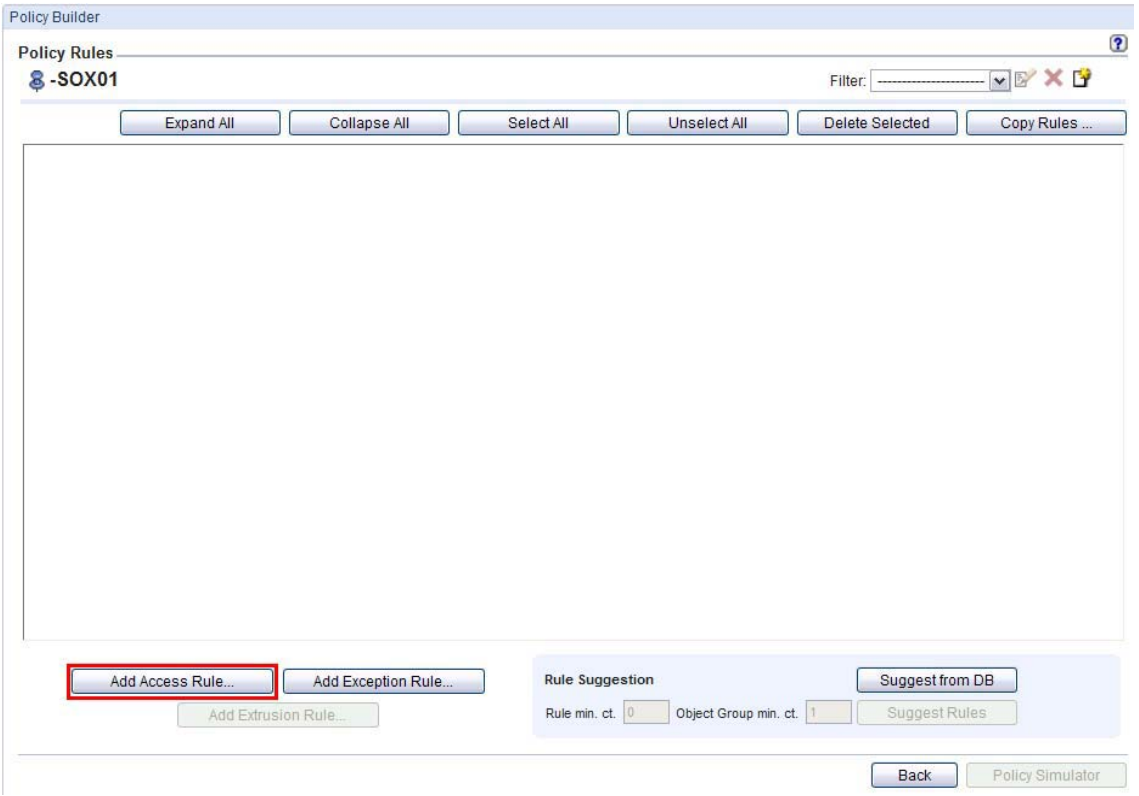
Figure 9-17. Policy Definition (2 of 2) GU2022.0

Notes:

- The **Roles…** button allows you to grant access to other users.
- **Back** will bring you back to the previous screen
- **Edit Rules…** will take you to the next step in creating your policy
- **Apply** saves the policy definition

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Policy Rules



© Copyright IBM Corporation 2011, 2013

Figure 9-18. Policy Rules GU2022.0

Notes:

Next, you start adding your rules to the policy. There are three types of rules to choose from:

- **Access Rule** – SQL requests made by client against a database server
- **Exception Rule** – SQL Errors and Failed login messages returned by the database server to the client
- **Extrusion** – Result sets returned by the database server to the client

We will start with Access Rules, followed by Exception and Extrusion rules. Pressing **Add Access Rule…** will allow you to create a new Access Rule, as shown in the next topic.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. Which of the following is NOT a built-in policy in Guardium?
    1. HIPAA
    2. BASEL II
    3. PCI
    4. SOX
    5. ACCT IV

2. Result sets would be part of an _____ rule.

3. Failed logins would be part of an _____ rule.

4. SELECTS would be part of an _____ rule.

© Copyright IBM Corporation 2011, 2013

Figure 9-19. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. Which of the following is NOT a built-in policy in Guardium?
   a. HIPAA
   b. BASEL II
   c. PCI
   d. SOX
   e. **ACCT IV**
2. Result sets would be part of an **extrusion** rule.
3. Failed logins would be part of an **exception** rule.
4. SELECTS would be part of an **access** rule.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Install a policy
- Access the policy builder
- Create a new policy

© Copyright IBM Corporation 2011, 2013

Figure 9-20. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. Which of the following is NOT a built-in policy in Guardium?
   1. HIPAA
   2. BASEL II
   3. PCI
   4. SOX
   5. **ACCT IV**
2. Result sets would be part of an **extrusion** rule.
3. Failed logins would be part of an **exception** rule.
4. SELECTS would be part of an **access** rule.

© Copyright IBM Corporation 2011, 2013

Figure 9-21. Checkpoint solutions GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- You can complete **Exercise 6** in the Exercise Guide. Alternately, you can wait and do Exercises 6 and 7 at the end of this unit.

© Copyright IBM Corporation 2011, 2013

Figure 9-22. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

9.3. Access Rules

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access rules

After completing this topic, you should be able to:

- Create access rules within a policy

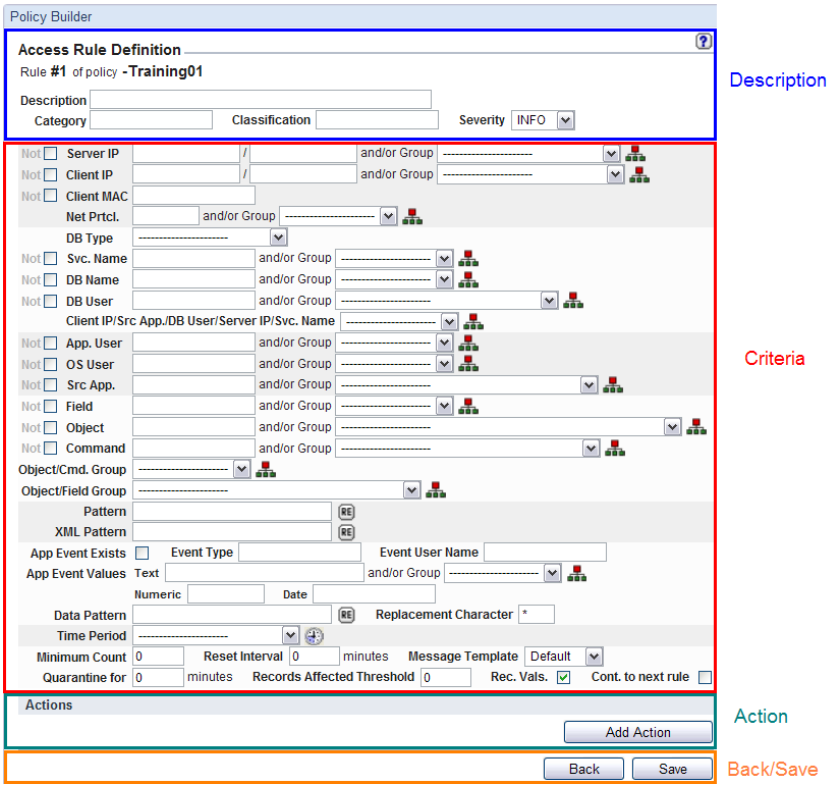
© Copyright IBM Corporation 2011, 2013

Figure 9-23. Access rules GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Overview



© Copyright IBM Corporation 2011, 2013

Figure 9-24. Access Rule: Overview GU2022.0

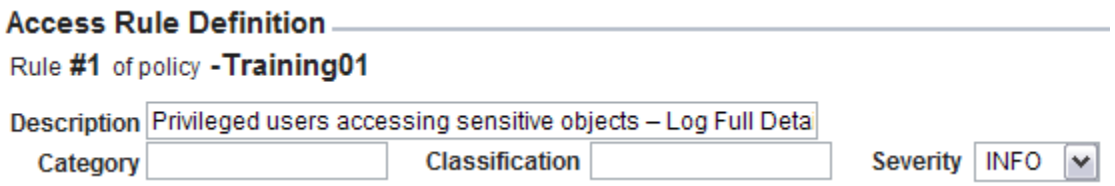
Notes:

A policy rule is made up of four sections

- **Rule Description** – Explains the purpose of the policy rule
- **Criteria** – Defines the fields and options that will trigger the rule
- **Action** – The activity that the appliance will perform when a rule is triggered
- **Back/Save** – Allows you to save or discard the policy rule

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Description



© Copyright IBM Corporation 2011, 2013

Figure 9-25. Access Rule: Description GU2022.0

Notes:

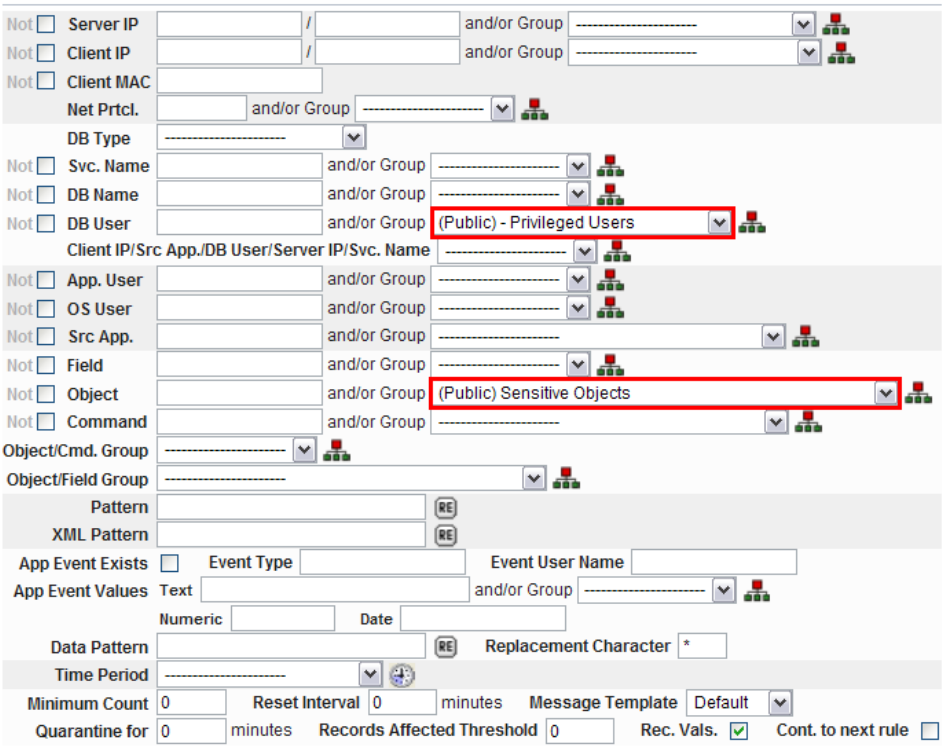
- **Rule Description** – Use this to describe what the rule does. This will be displayed in any policy rule violation.
- **Category** - The category will be logged with violations, and is used for grouping and reporting purposes. If nothing is entered, the default for the policy will be used.
- **Classification** - Optionally enter a classification in the Classification box. Like the category (above), these are logged with exceptions and can be used for grouping and reporting purposes.
- **Severity** - Select a severity code: Info, Low, Med, or High (the default is Info).

The Rule Description is the only required field.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Criteria


Not Server IP / and/or Group
Not Client IP / and/or Group
Not Client MAC
Net Prtcl. and/or Group
DB Type
Not Svc. Name and/or Group
Not DB Name and/or Group
Not DB User and/or Group (Public) - Privileged Users
Client IP/Src App./DB User/Server IP/Svc. Name
Not App. User and/or Group
Not OS User and/or Group
Not Src App. and/or Group
Not Field and/or Group
Not Object and/or Group (Public) Sensitive Objects
Not Command and/or Group
Object/Cmd. Group
Object/Field Group
Pattern
XML Pattern
App Event Exists Event Type Event User Name
App Event Values Text and/or Group
Numeric Date
Data Pattern Replacement Character *
Time Period
Minimum Count 0 Reset Interval 0 minutes Message Template Default
Quarantine for 0 minutes Records Affected Threshold 0 Rec. Vals. Cont. to next rule

© Copyright IBM Corporation 2011, 2013

Figure 9-26. Access Rule: Criteria GU2022.0

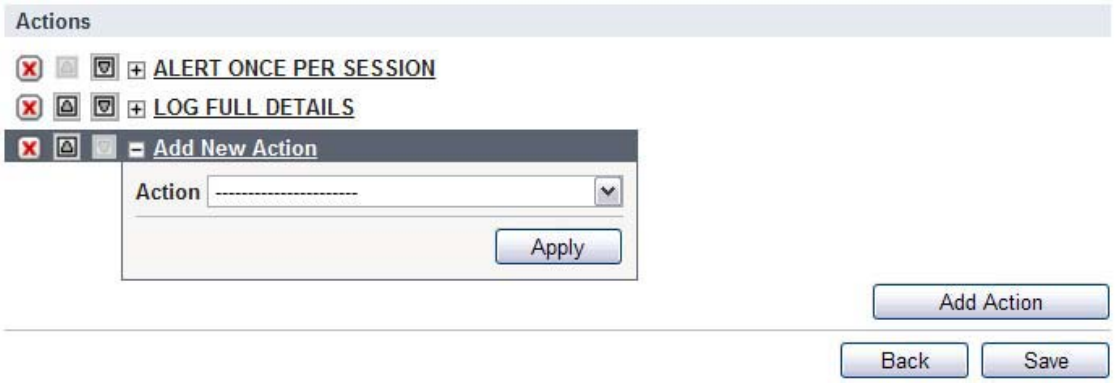
Notes:

All of the fields from **Server IP** through **Records Affected Threshold** make up the criteria of the rule.

- If you choose fields in separate rows, both conditions must be satisfied for the rule to trigger (**AND Conditions**). In the example above, the user must be in the *Privileged Users* group and the object must be in the *Sensitive Objects* group for the rule to fire.
- (**OR** Condition) If you choose two fields within the same row, a match for either will satisfy that criterion; Object = *cc_numbers* OR Object IN GROUP *Sensitive Objects*.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Action and Back/Save



© Copyright IBM Corporation 2011, 2013

Figure 9-27. Access Rule: Action and Back/Save GU2022.0

Notes:

Actions

The actions section allows you to specify the resulting activity when the rule's criteria has been met. One rule may contain multiple actions. To add an action, choose the name from the pull down list and press **Apply**. When you have added all of the actions that you require, press the **Add Action** button.

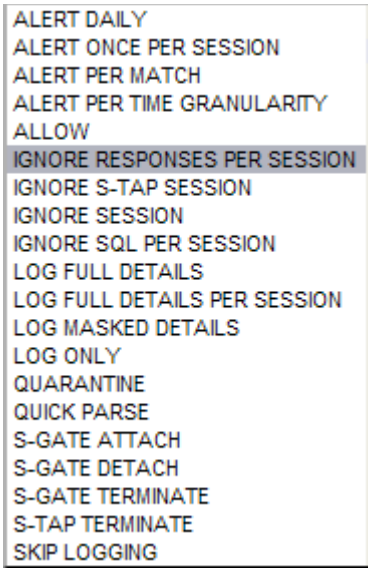
Back / Save

The **Back** and **Save** buttons allow you to discard or save an changes made to the rule.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Actions



© Copyright IBM Corporation 2011, 2013

Figure 9-28. Access Rule: Actions GU2022.0

Notes:

Access rules fall into these categories:

Alerts/Policy Violations

- ALERT DAILY
- ALERT ONCE PER SESSION
- ALERT PER MATCH
- ALERT PER TIME GRANUALITY
- LOG ONLY

Filters

- IGNORE RESPONSES PER SESSION
- IGNORE S-TAP SESSION
- IGNORE SESSION
- IGNORE SQL PER SESSION

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- SKIP LOGGING

Log Full Details Rules

- LOG FULL DETAILS
- LOG FULL DETAILS PER SESSION
- LOG MASKED DETAILS

Firewall/Blocking

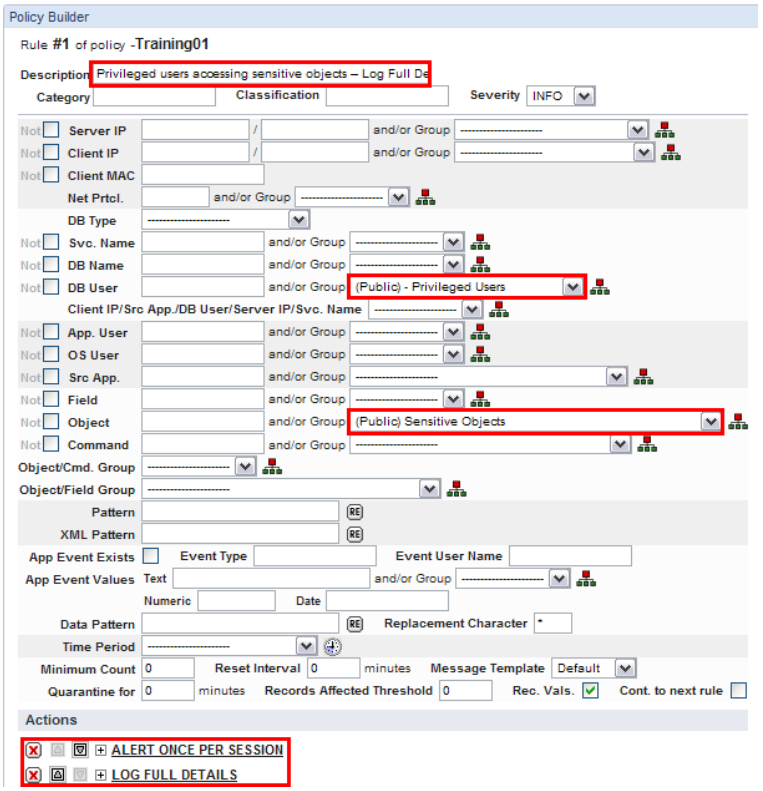
- QUARANTINE
- S-GATE ATTACH
- S-GATE DETATCH
- S-GATE TERMINATE
- S-TAP TERMINATE

Other Logging Rules

- ALLOW
- QUICK PARSE

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access Rule: Example



© Copyright IBM Corporation 2011, 2013

Figure 9-29. Access Rule: Example GU2022.0

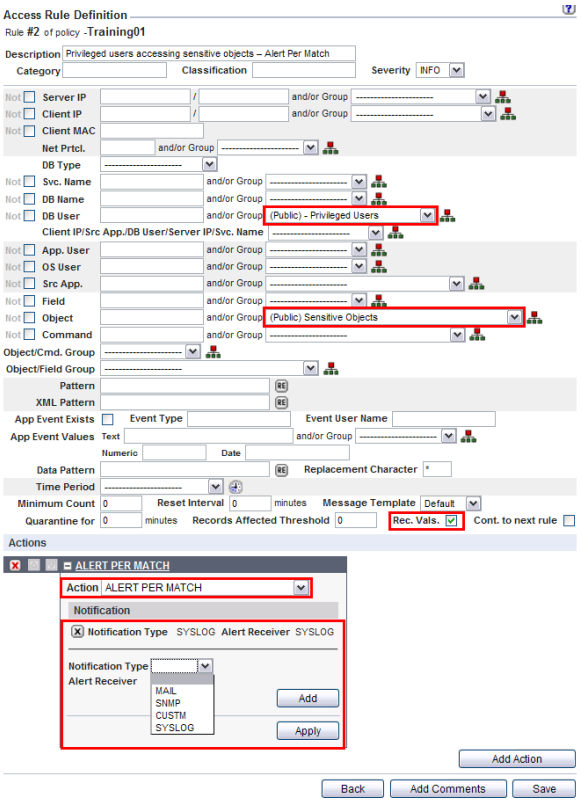
Notes:

This is an example of a complete Access rule:

- **Description** – *Privileged users accessing sensitive objects – Log Full Details*
- **Criteria** – DB User IN GROUP *Privileged Users* AND Object IN GROUP *Sensitive Objects*
- **Actions** – *Alert Once Per Session* AND *Log Full Details*

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Alert rules



© Copyright IBM Corporation 2011, 2013

Figure 9-30. Alert rules GU2022.0

Notes:

Alert rules will send a notification to designated receivers at a defined frequency, depending on the action chosen.

Actions

- **Alert Daily** sends notifications only the first time the rule is matched each day.
- **Alert Once Per Session** sends notifications only once for each session in which the rule is matched.
- **Alert Per Match** sends notifications each time the rule is satisfied.
- **Alert Per Time Granularity** sends notifications once per logging granularity period. For example, if the logging granularity is set to one hour, notifications will be sent for only the first match for the rule during each hour.

Receivers

- **Email messages**, which must be addressed to Guardium users, and will be sent via the SMTP server configured for Guardium.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **SNMP traps**, which will be sent to the trap community configured for the Guardium appliance.
- **Syslog messages**, which will be written to syslog. This is commonly used to a SIEM, such as Tivoli Security Operations Manager
- **Custom notifications**, which are user-written notification handlers, implemented as Java classes.

Rec Values

- The Record Values check box, indicates whether the full, unmasked, SQL string will be included with the alert.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Alert example

```
db2 => connect to localtcp user a8000 using a8000abc

   Database Connection Information

 Database server        = DB2/LINUX 9.7.1
 SQL authorization ID   = A8000
 Local database alias   = LOCALTCP

db2 => select * from db2inst1.g employees

E_ID        E_FIRSTNAME                E_LASTNAME
----------- -------------------------- ----------------
       1001 Henry                      Xavier

  1 record(s) selected.
```

```
Oct 20 14:00:56 grd01 guard_sender[3326]: Alert based on rule ID Privileged us
ers accessing sensitive objects â Alert Per Match#012Category:   Classificatio
n:    Severity INFO  #012Rule # 20001 [Privileged users accessing sensitive ob
jects â Alert Per Match ]#012Request Info: [ Session start: 2010-10-20#01113:5
4:56 Server Type: DB2 Client: 192.168.169.8 (DBSERVER01) Server: 192.168.169.8
 () Client PORT: 39442 Server Port: 50001 Service Name: DB2INST1 Net Protocol:
 TCP DB Protocol: DRDA DB Protocol Version: 3.0 DB User: A8000#012Application
User Name  #012Source Program: DB2BP Authorization Code: 0 Request Type: SQL_L
ANG Last Error: #012SQL: select * from db2inst1.g employees#012 To add to base
line:
```

© Copyright IBM Corporation 2011, 2013

Figure 9-31. Alert example GU2022.0

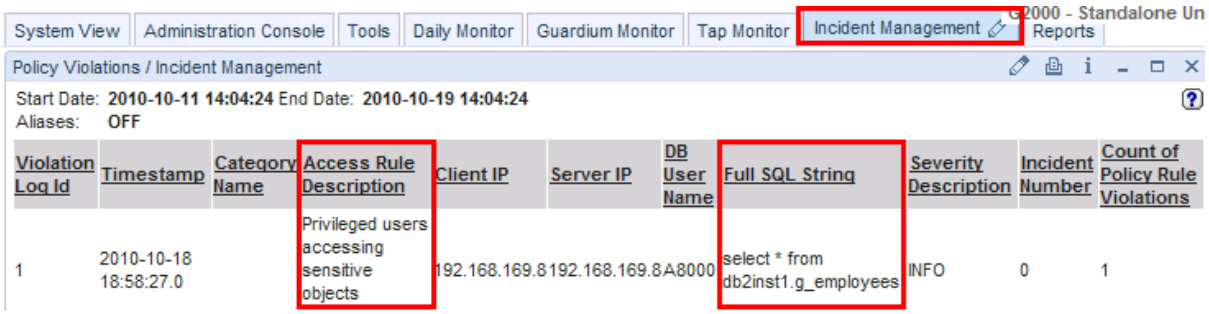
Notes:

This is an example of a triggered alert going to syslog. Note that the alert contains the policy rule name and it includes the full SQL statement because the *Rec Values* box was checked.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Policy violation

```
db2 => connect to localtcp user a8000 using a8000abc

   Database Connection Information

 Database server        = DB2/LINUX 9.7.1
 SQL authorization ID   = A8000
 Local database alias   = LOCALTCP

db2 => select * from db2inst1.g employees

E_ID        E_FIRSTNAME                E_LASTNAME
----------- -------------------------- ----------------
       1001 Henry                      Xavier

  1 record(s) selected.
```



© Copyright IBM Corporation 2011, 2013

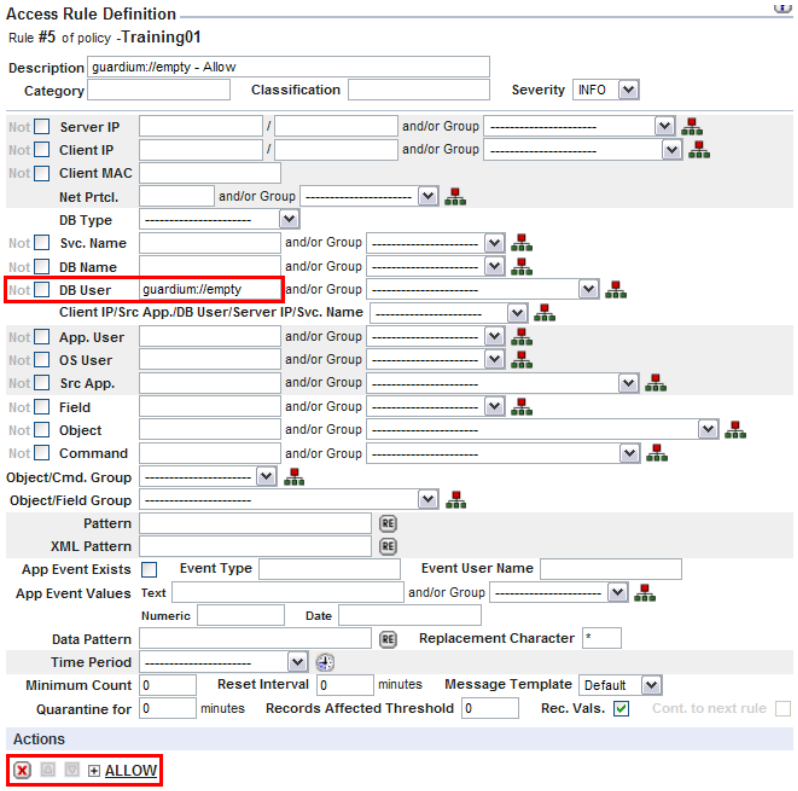
Figure 9-32. Policy violation GU2022.0

Notes:

When an alert rule is triggered, the appliance will also log a *Policy Violation*. The **Incident Management** tab is an easily accessible location to view all policy violations.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Allow



© Copyright IBM Corporation 2011, 2013

Figure 9-33. Allow GU2022.0

Notes:

With multiple rules in a policy, the rules are processed from top to bottom. When a rule is triggered, the default behavior is to stop processing subsequent rules, unless the *Cont to next rule* box is checked.

The **Allow** action serves to help control this flow. The Allow rule informs the sniffer to log the traffic normally (log the construct and Access Period timestamp) and to not continue to the next rule (note that the *Continue to next rule* checkbox is grayed out and unavailable). This is commonly used when you would like to prevent certain activity from reaching specific rules further down in the policy.

A real-world example of when this rule is used is when a customer requirement is to log activity by *privileged users* only for MS SQL Server 2005 or 2008 database servers. To meet such a requirement, you would normally create a rule specifying 'if the user is NOT in the *Privileged User* group, ignore session'. With most database types, this rule would be sufficient. However, with MS SQL Server 2005/2008, many login packets are encrypted and it takes Guardium a few seconds to resolve the encrypted login to the actual user name. While the resolution is taking place the user name appears as an empty string and,

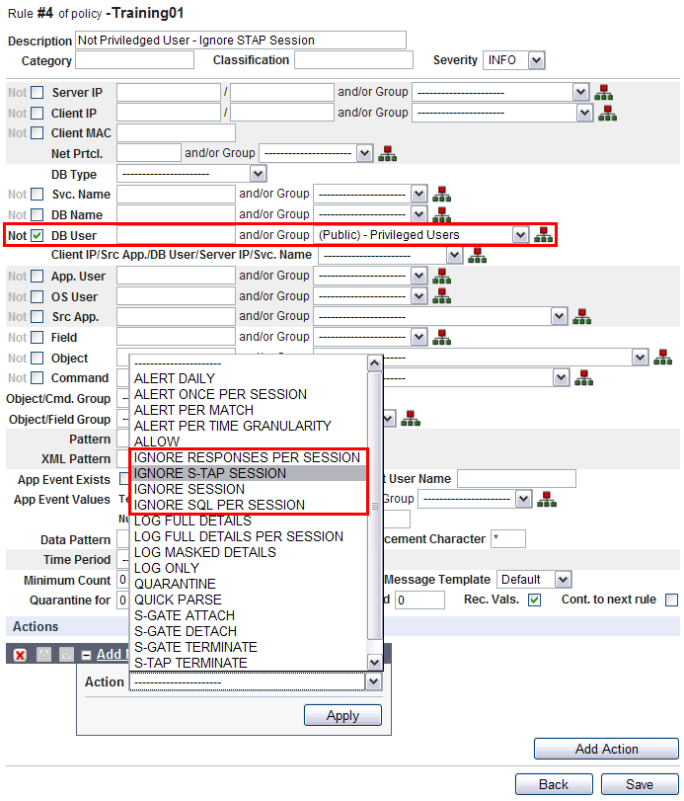
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

being empty, it would not be in the *Privileged User* group and would, thus, be ignored. To prevent privileged user sessions from being ignored incorrectly, you would add an **Allow** rule with a special **guardium://empty** flag in the DB User field before the *Ignore Session* rule. While the user name is empty, the traffic will be logged normally. When the user name is resolved, this rule would not be triggered because it will not longer be empty, allowing the session to be evaluated by the *Ignore Session* rule.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore session rules



© Copyright IBM Corporation 2011, 2013

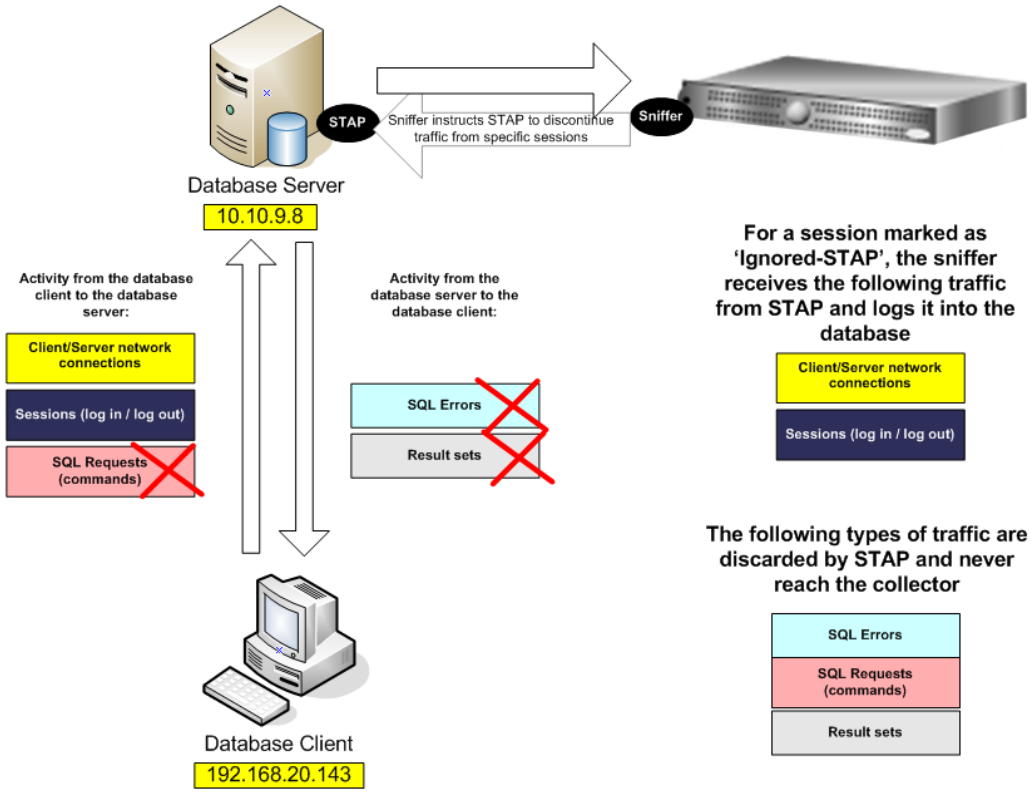
Figure 9-34. Ignore session rules GU2022.0

Notes:

Ignore Session rules provide the most effective method of filtering traffic. An ignore session rule will cause activity from individual sessions to be dropped by the STAP or completely ignored by the sniffer. Note: connection (login/logout) information is always logged, even if the session is ignored.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore STAP session


STAP
Sniffer instructs STAP to discontinue traffic from specific sessions
Sniffer
Database Server
10.10.9.8
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
SQL Errors
Result sets
For a session marked as 'Ignored-STAP', the sniffer receives the following traffic from STAP and logs it into the database
Client/Server network connections
Sessions (log in / log out)
The following types of traffic are discarded by STAP and never reach the collector
SQL Errors
SQL Requests (commands)
Result sets
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

Figure 9-35. Ignore STAP session GU2022.0

Notes:

The 'Ignore STAP session' action follows this process:

1. The user logs into the database server
2. STAP sends the connection information, along with the first few commands, to the sniffer
3. The sniffer determines based on the policy rule that the session should be ignored
4. The sniffer sends a signal to STAP to stop sending traffic from that session
5. STAP discontinues sending traffic from the session
6. The user logs out of the database
7. STAP sends the logout packet to the sniffer

- If STAP continues to send traffic from a session that should be ignored, the sniffer will continue to send the signal to STAP to ignore the session.

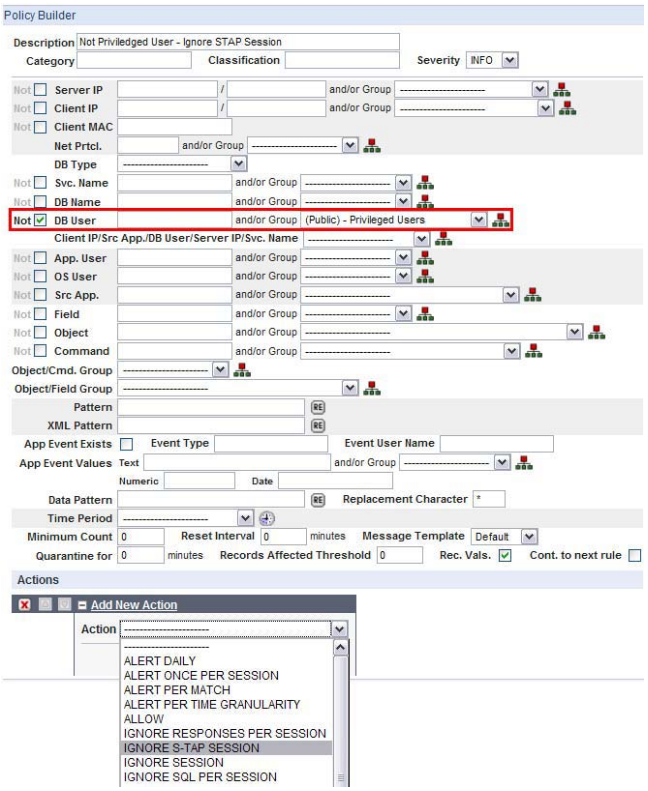
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- The process described above is repeated for every connection; this keeps resource utilization as low as possible on the database server. All policy logic is maintained by the collector while STAP only maintains the list of sessions to be ignored.
- If you have an STAP-only environment, use the *Ignore STAP Session* rule, not *Ignore Session*, to completely ignore a session. *Ignore Session* only sends the 'ignore' signal to STAP once and is not as robust as *Ignore STAP Session*. However, if you use a SPAN Port or Network TAP, you would need to use *Ignore Session* rules for network traffic.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Ignore STAP Session rule



© Copyright IBM Corporation 2011, 2013

Figure 9-36. Ignore STAP Session rule GU2022.0

Notes:

In the example above, all sessions will be ignored, except for those in the *Privileged Users* group.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore sessions and sizing

Ignored session rules can positively affect:

- The number of collectors required
- The performance of each collector
- Data retention

© Copyright IBM Corporation 2011, 2013

Figure 9-37. Ignore sessions and sizing GU2022.0

Notes:

Choosing which sessions to be ignored depends on how the Guardium solution was sized in the sales process. For example, some implementations are defined as ‘Privileged user only’. In this situation the customer will define a group of privileged users and create a rule to *Ignore STAP Session* when the user is not in the group of privileged users. Other implementations are defined as comprehensive in which all (or almost all) sessions are logged. Most implementations fall somewhere in between; more than just privileged users will be logged but many trusted sessions (applications, backups, scheduled processes, etc.) can be ignored.

The ignore session rules have a great impact on the performance of the collector and data retentions. If you log privileged user activity only, you would require less collectors than a ‘comprehensive’ implementation, in which all traffic is logged.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore STAP session rule: Trusted connections

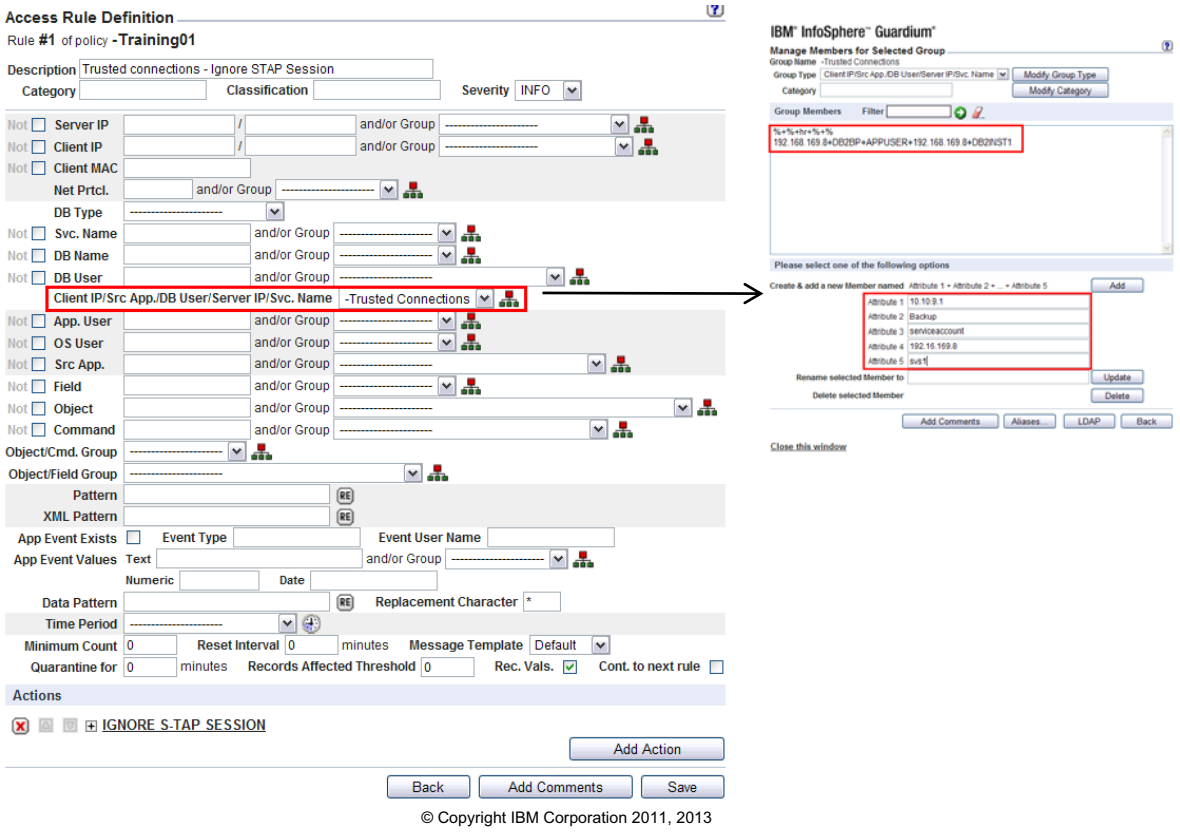


Figure 9-38. Ignore STAP session rule: Trusted connections GU2022.0

Notes:

The **Client IP/Src App./DB User/Server IP/Svc. Name** group allows you to specify the exact sessions that you would like to ignore. For example, activity from a service account on an application server using a specific application can be ignore but if the connection does not meet all three criteria the activity should be logged.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Trusted connections group

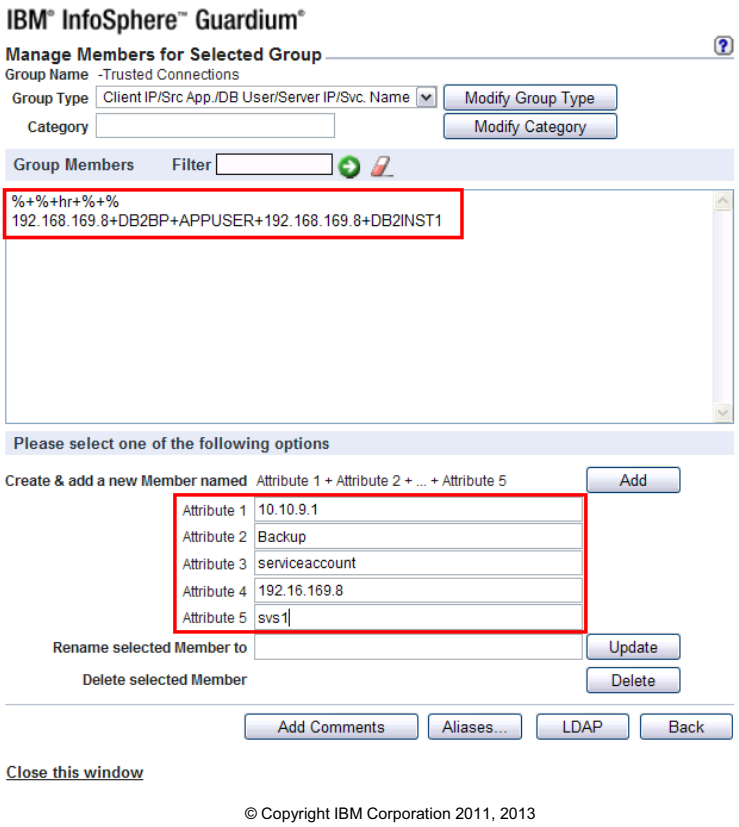


Figure 9-39. Trusted connections group GU2022.0

Notes:

The **Client IP/Src App./DB User/Server IP/Svc. Name** group contains five attributes that should be added in this order:

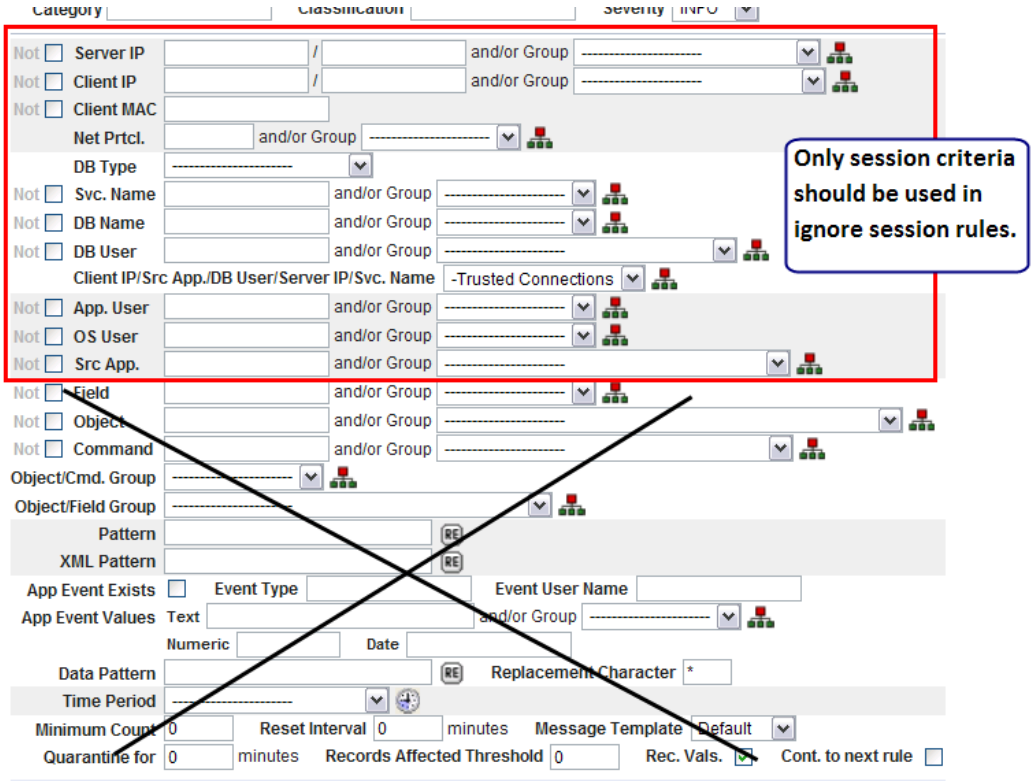
- Attributive 1 = Client IP
- Attributive 2 = Src App.
- Attributive 3 = DB User
- Attributive 4 = Server IP
- Attributive 5 = Svc. Name

A wildcard (%) can be added, if a specific attribute is not relevant.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore session criteria



© Copyright IBM Corporation 2011, 2013

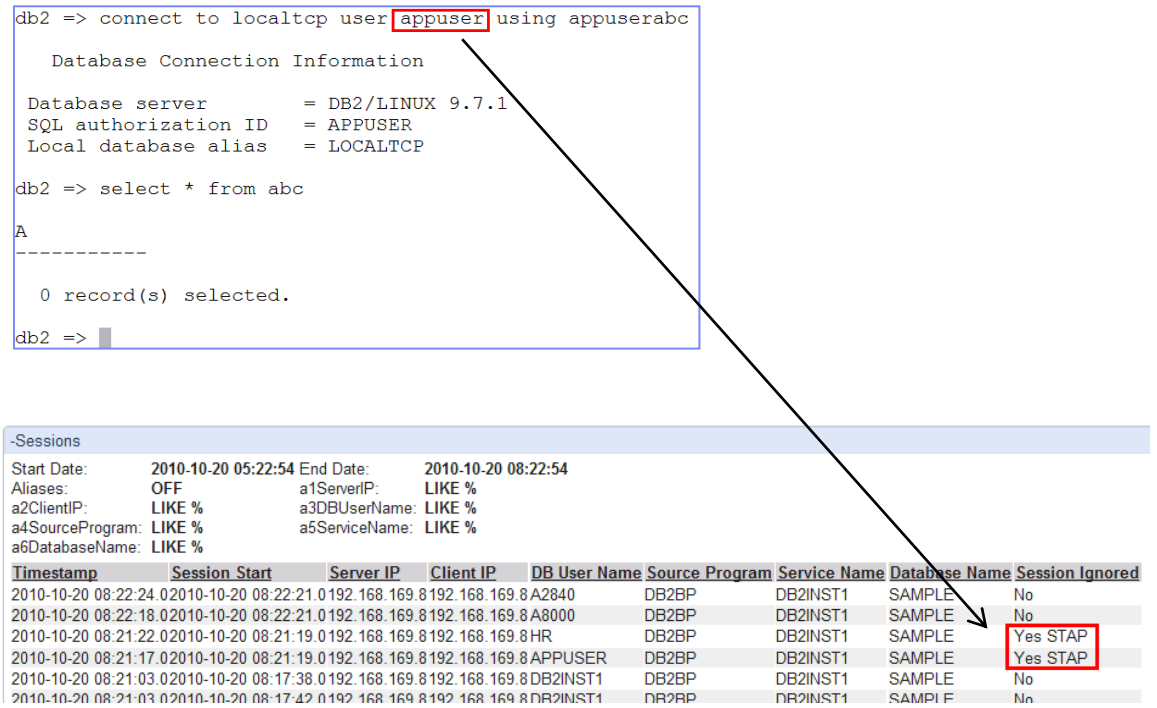
Figure 9-40. Ignore session criteria GU2022.0

Notes:

All ***Ignore Session*** actions should only have session-based fields as criteria otherwise you will experience unexpected results.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore STAP session example


db2 => connect to localtcp user appuser using appuserabc
Database Connection Information
Database server = DB2/LINUX 9.7.1
SQL authorization ID = APPUSER
Local database alias = LOCALTCP
db2 => select * from abc
A
0 record(s) selected.
db2 =>
-Sessions
Start Date: 2010-10-20 05:22:54 End Date: 2010-10-20 08:22:54
Aliases: OFF a1ServerIP: LIKE %
a2ClientIP: LIKE % a3DBUserName: LIKE %
a4SourceProgram: LIKE % a5ServiceName: LIKE %
a6DatabaseName: LIKE %
Timestamp Session Start Server IP Client IP DB User Name Source Program Service Name Database Name Session Ignored
2010-10-20 08:22:24.0 2010-10-20 08:22:21.0 192.168.169.8 192.168.169.8 A2840 DB2BP DB2INST1 SAMPLE No
2010-10-20 08:22:18.0 2010-10-20 08:22:21.0 192.168.169.8 192.168.169.8 A8000 DB2BP DB2INST1 SAMPLE No
2010-10-20 08:21:22.0 2010-10-20 08:21:19.0 192.168.169.8 192.168.169.8 HR DB2BP DB2INST1 SAMPLE Yes STAP
2010-10-20 08:21:17.0 2010-10-20 08:21:19.0 192.168.169.8 192.168.169.8 APPUSER DB2BP DB2INST1 SAMPLE Yes STAP
2010-10-20 08:21:03.0 2010-10-20 08:17:38.0 192.168.169.8 192.168.169.8 DB2INST1 DB2BP DB2INST1 SAMPLE No

© Copyright IBM Corporation 2011, 2013

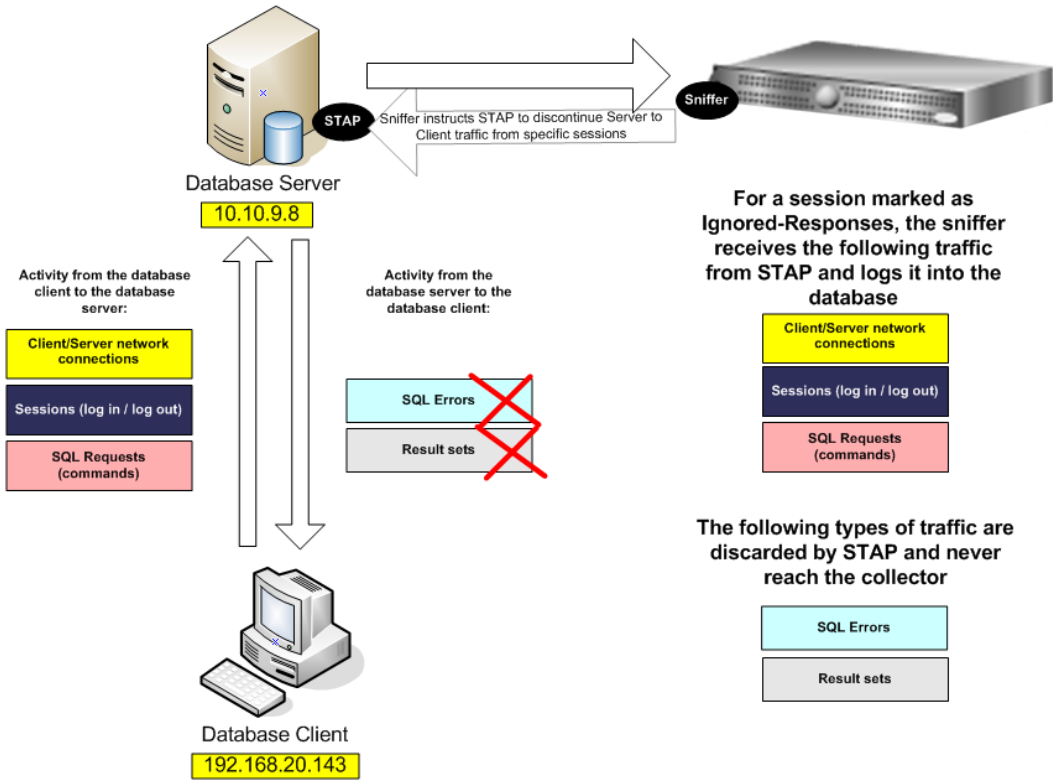
Figure 9-41. Ignore STAP session example GU2022.0

Notes:

To confirm that an Ignore STAP Session works properly, create a report with the *Session Ignored* flag. This report is included on the training machines.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore responses per session


STAP
Sniffer instructs STAP to discontinue Server to Client traffic from specific sessions
Sniffer
Database Server
10.10.9.8
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
SQL Errors
Result sets
For a session marked as Ignored-Responses, the sniffer receives the following traffic from STAP and logs it into the database
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
The following types of traffic are discarded by STAP and never reach the collector
SQL Errors
Result sets
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

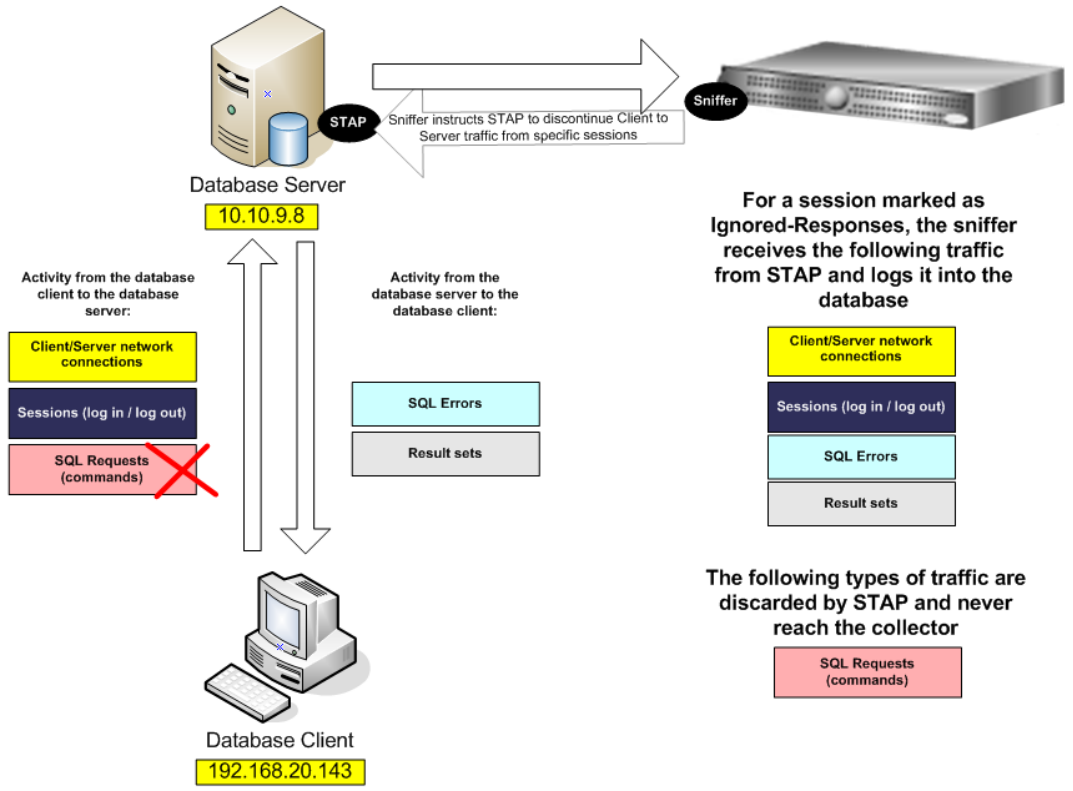
Figure 9-42. Ignore responses per session GU2022.0

Notes:

The *Ignore Responses Per Session* action will cause the collector to continue logging SQL Requests but the sniffer will instruct STAP to discontinue forwarding responses from the DB Server to the client. Responses include SQL Errors and Result Sets.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore SQL per session


STAP
Sniffer instructs STAP to discontinue Client to Server traffic from specific sessions
Sniffer
Database Server
10.10.9.8
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
SQL Errors
Result sets
For a session marked as Ignored-Responses, the sniffer receives the following traffic from STAP and logs it into the database
Client/Server network connections
Sessions (log in / log out)
SQL Errors
Result sets
The following types of traffic are discarded by STAP and never reach the collector
SQL Requests (commands)
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

Figure 9-43. Ignore SQL per session GU2022.0

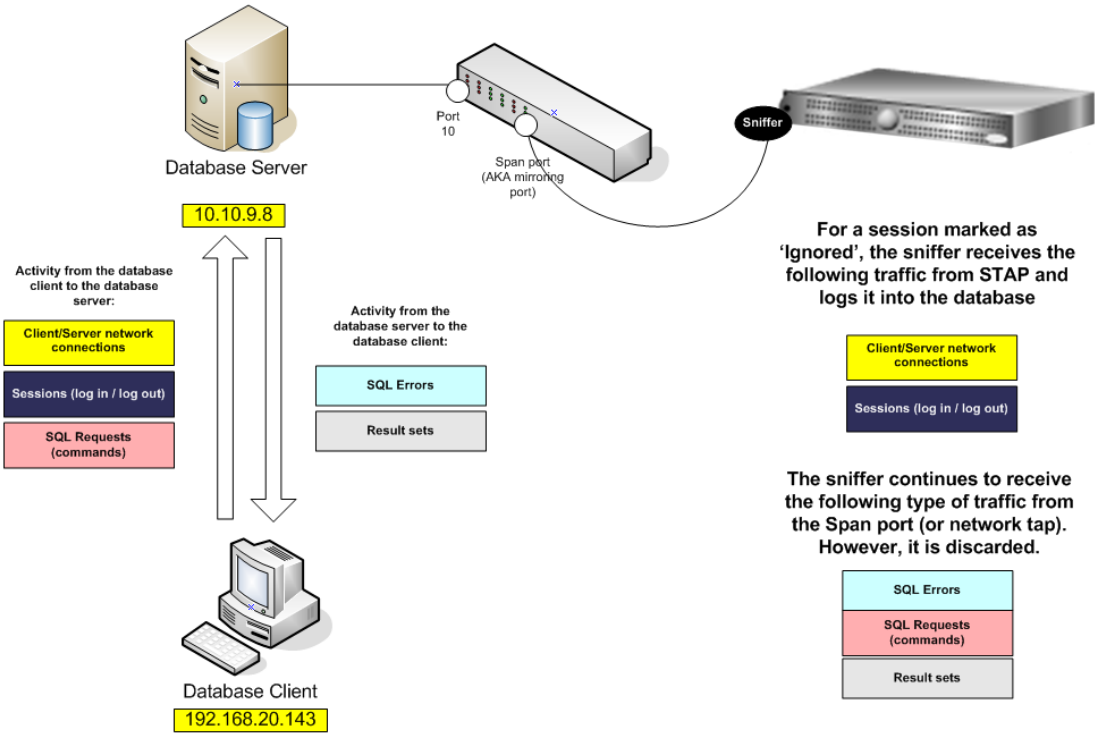
Notes:

The *Ignore SQL Per Session* action will cause the collector to continue logging SQL Errors and Result Sets but the sniffer will instruct STAP to discontinue forwarding SQL requests from the client to the database server.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Ignore session


Database Server
10.10.9.8
Port 10
Span port (AKA mirroring port)
Sniffer
For a session marked as 'Ignored', the sniffer receives the following traffic from STAP and logs it into the database
Client/Server network connections
Sessions (log in / log out)
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
SQL Errors
Result sets
The sniffer continues to receive the following type of traffic from the Span port (or network tap). However, it is discarded.
SQL Errors
SQL Requests (commands)
Result sets
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

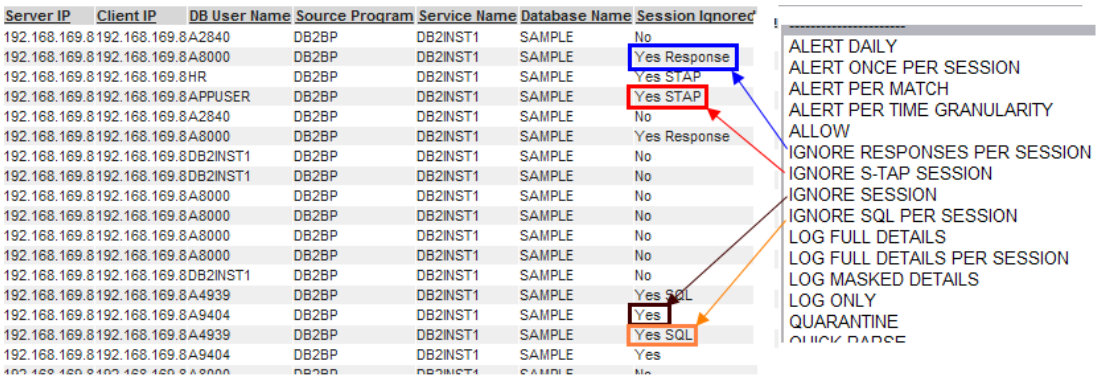
Figure 9-44. Ignore session GU2022.0

Notes:

The *Ignore Session* rule should only be used when a hardware solution (span ports or network taps) is used to capture traffic. In this instance, all traffic reaches the sniffer, which then discards it.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Session ignored values



Server IP	Client IP	DB User Name	Source Program	Service Name	Database Name	Session Ignored
192.168.169.8	192.168.169.8	A2840	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	Yes Response
192.168.169.8	192.168.169.8	HR	DB2BP	DB2INST1	SAMPLE	Yes STAP
192.168.169.8	192.168.169.8	APPUSER	DB2BP	DB2INST1	SAMPLE	Yes STAP
192.168.169.8	192.168.169.8	A2840	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	Yes Response
192.168.169.8	192.168.169.8	DB2INST1	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	DB2INST1	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A8000	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	DB2INST1	DB2BP	DB2INST1	SAMPLE	No
192.168.169.8	192.168.169.8	A4939	DB2BP	DB2INST1	SAMPLE	Yes SQL
192.168.169.8	192.168.169.8	A9404	DB2BP	DB2INST1	SAMPLE	Yes
192.168.169.8	192.168.169.8	A4939	DB2BP	DB2INST1	SAMPLE	Yes SQL
192.168.169.8	192.168.169.8	A9404	DB2BP	DB2INST1	SAMPLE	Yes

© Copyright IBM Corporation 2011, 2013

Figure 9-45. Session ignored values GU2022.0

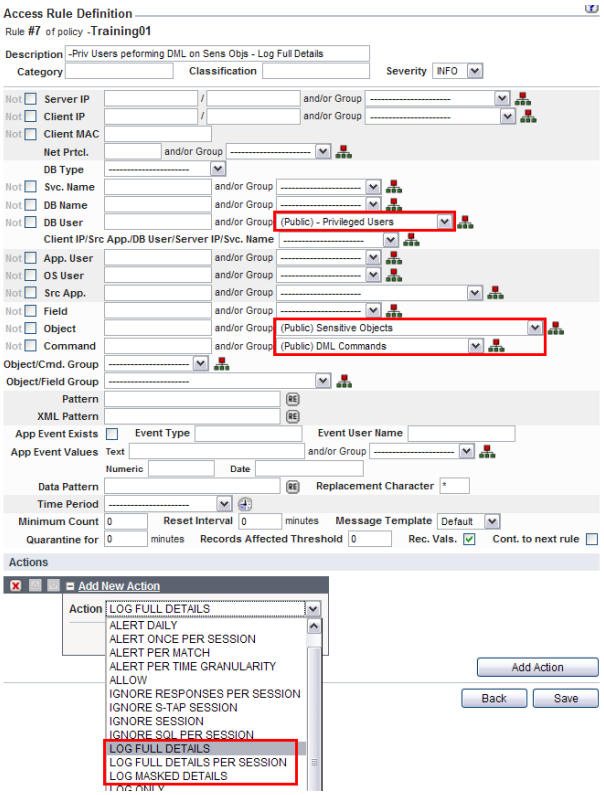
Notes:

Each *Ignore Session* rule type has its own flag in the *Session Ignored* field.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log full details



© Copyright IBM Corporation 2011, 2013

Figure 9-46. Log full details GU2022.0

Notes:

To meet some customer requirements, logging just the construct would not be sufficient. For these cases, Guardium has the ability to log more than the construct, using the ‘Log Full Details’ policy action.

With some variation the ‘Log Full Details’ actions:

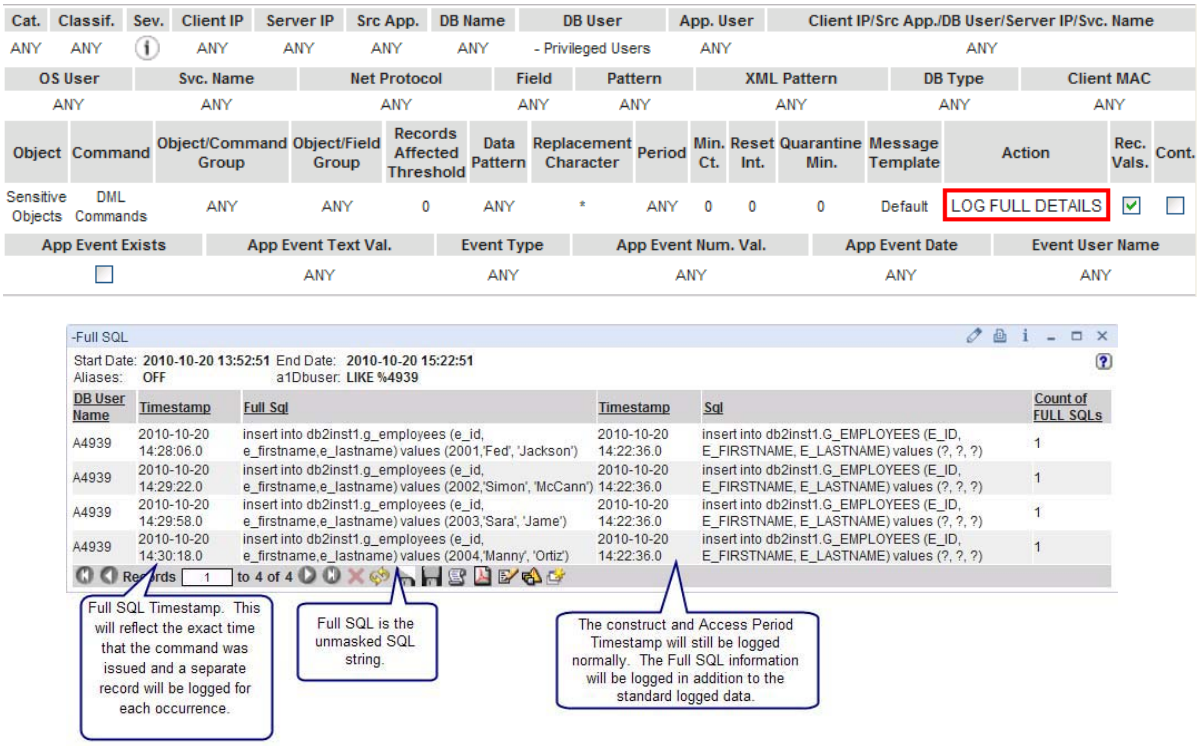
- Log the exact timestamp for each occurrence matching the rule criteria
- Log the unmasked, full, SQL string executed by the user

Examples of when Log Full Details rules are appropriate:

- The exact timestamp is required
- The values entered in a SQL request are of interest

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log full details: Example


Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User Client IP/Src App./DB User/Server IP/Svc. Name
ANY ANY ANY ANY ANY - Privileged Users ANY ANY
OS User Svc. Name Net Protocol Field Pattern XML Pattern DB Type Client MAC
ANY ANY ANY ANY ANY ANY ANY ANY
Object Command Object/Command Group Object/Field Group Records Affected Threshold Data Pattern Replacement Character Period Min. Ct. Reset Int. Quarantine Min. Message Template Action Rec. Vals. Cont.
Sensitive Objects DML Commands ANY ANY 0 ANY * ANY 0 0 0 Default LOG FULL DETAILS
App Event Exists App Event Text Val. Event Type App Event Num. Val. App Event Date Event User Name
ANY ANY ANY ANY ANY
-Full SQL
Start Date: 2010-10-20 13:52:51 End Date: 2010-10-20 15:22:51
Aliases: OFF a1Dbuser: LIKE %4939
DB User Name Timestamp Full Sql Timestamp Sql Count of FULL SQLs
A4939 2010-10-20 14:28:06.0 insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (2001,'Fed', 'Jackson') 2010-10-20 14:22:36.0 insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?) 1
A4939 2010-10-20 14:29:22.0 insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (2002,'Simon', 'McCann') 2010-10-20 14:22:36.0 insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?) 1
A4939 2010-10-20 14:29:58.0 insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (2003,'Sara', 'Jame') 2010-10-20 14:22:36.0 insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?) 1
A4939 2010-10-20 14:30:18.0 insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (2004,'Manny', 'Ortiz') 2010-10-20 14:22:36.0 insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?) 1
Records 1 to 4 of 4
Full SQL Timestamp. This will reflect the exact time that the command was issued and a separate record will be logged for each occurrence.
Full SQL is the unmasked SQL string.
The construct and Access Period Timestamp will still be logged normally. The Full SQL information will be logged in addition to the standard logged data.

© Copyright IBM Corporation 2010,2013

Figure 9-47. Log full details: Example GU2022.0

Notes:

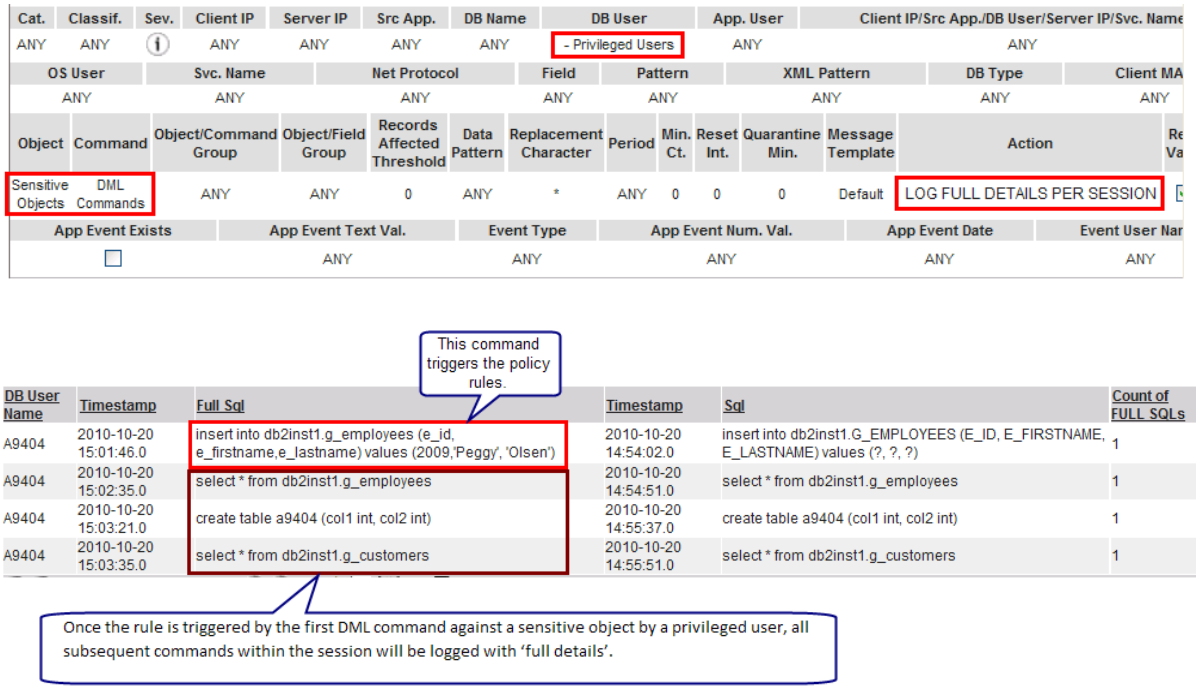
When the **Log Full Details** action is triggered, each individual SQL request will be logged into the *Full SQL* entity with the exact time the command was issued and the full, unmasked SQL string. The constructs and Access Period timestamps will also still be logged normally.

Because each SQL request will now be logged, rather than just updating the construct counter, Log Full Details rules can potentially fill Guardium's internal database very quickly.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log full details per session



© Copyright IBM Corporation 2011, 2013

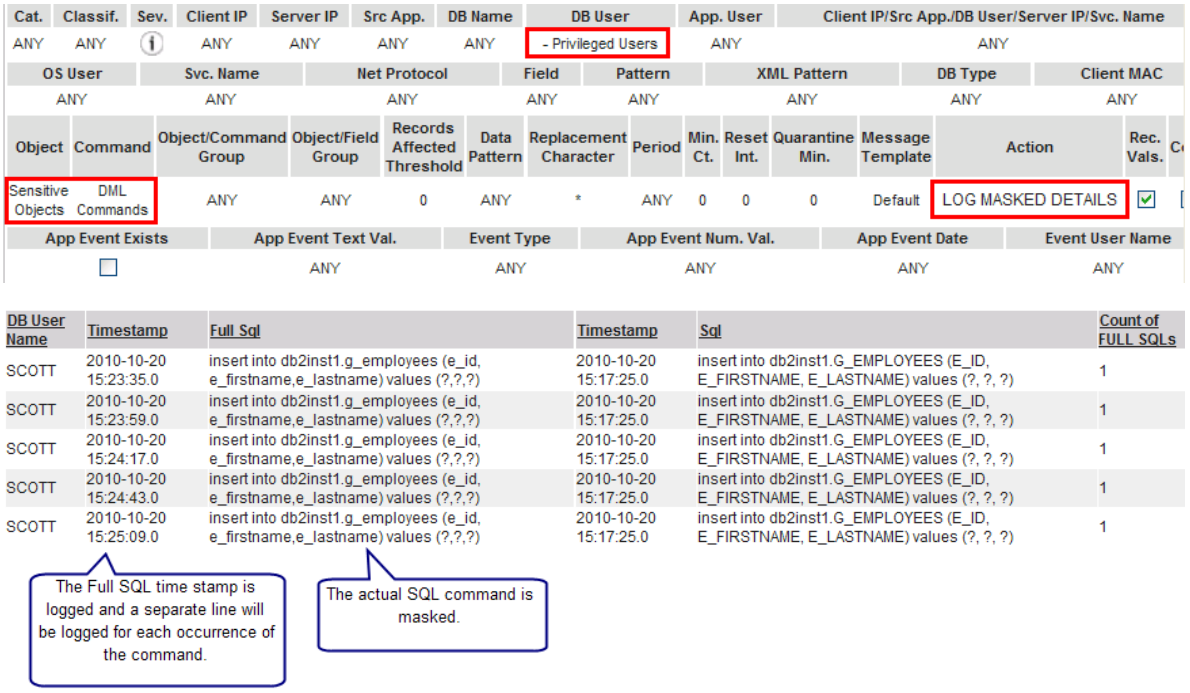
Figure 9-48. Log full details per session GU2022.0

Notes:

Log Full Details will log the Full SQL string and Full SQL Timestamp for only those SQL requests matching the rule criteria. *Log Full Details Per Session* will log the Full SQL string/Timestamp for the request that triggers the action AND all subsequent SQL request made during the remainder of the session.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log masked details



Cat.	Classif.	Sev.	Client IP	Server IP	Src App.	DB Name	DB User	App. User	Client IP/Src App./DB User/Server IP/Svc. Name
ANY	ANY		ANY	ANY	ANY	ANY	- Privileged Users	ANY	ANY

OS User	Svc. Name	Net Protocol	Field	Pattern	XML Pattern	DB Type	Client MAC
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Records Affected Threshold	Data Pattern	Replacement Character	Period	Min. Ct.	Reset Int.	Quarantine Min.	Message Template	Action	Rec. Vals.
Sensitive Objects	DML Commands	ANY	ANY	0	ANY	*	ANY	0	0	0	Default	LOG MASKED DETAILS	☑

App Event Exists	App Event Text Val.	Event Type	App Event Num. Val.	App Event Date	Event User Name
☐	ANY	ANY	ANY	ANY	ANY

DB User Name	Timestamp	Full Sql	Timestamp	Sql	Count of FULL SQLs
SCOTT	2010-10-20 15:23:35.0	insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (?,?,?)	2010-10-20 15:17:25.0	insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?)	1
SCOTT	2010-10-20 15:23:59.0	insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (?,?,?)	2010-10-20 15:17:25.0	insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?)	1
SCOTT	2010-10-20 15:24:17.0	insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (?,?,?)	2010-10-20 15:17:25.0	insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?)	1
SCOTT	2010-10-20 15:24:43.0	insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (?,?,?)	2010-10-20 15:17:25.0	insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?)	1
SCOTT	2010-10-20 15:25:09.0	insert into db2inst1.g_employees (e_id, e_firstname,e_lastname) values (?,?,?)	2010-10-20 15:17:25.0	insert into db2inst1.G_EMPLOYEES (E_ID, E_FIRSTNAME, E_LASTNAME) values (?, ?, ?)	1

The Full SQL time stamp is logged and a separate line will be logged for each occurrence of the command.
The actual SQL command is masked.

© Copyright IBM Corporation 2011, 2013

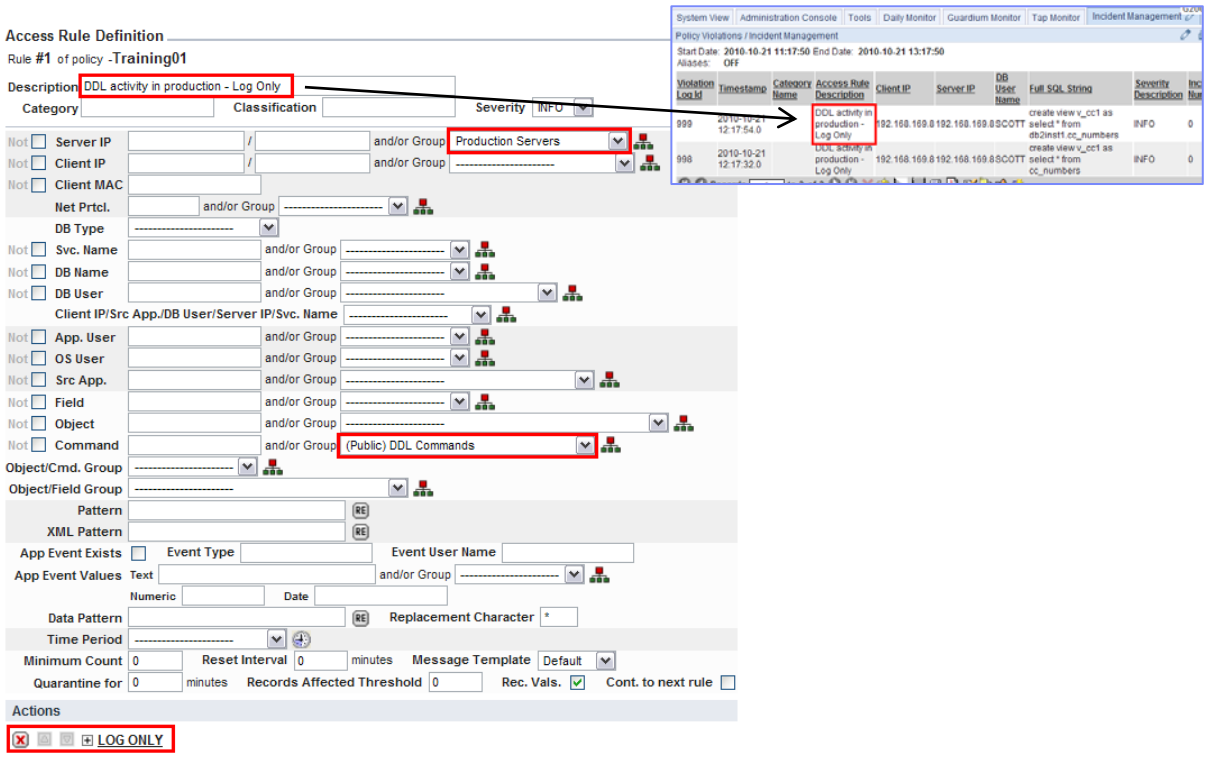
Figure 9-49. Log masked details GU2022.0

Notes:

Log Masked Details logs the Full SQL Timestamp but continues to mask the SQL string. This is used in instances where the exact time of SQL request is important but the values should not be exposed.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Log only



© Copyright IBM Corporation 2011, 2013

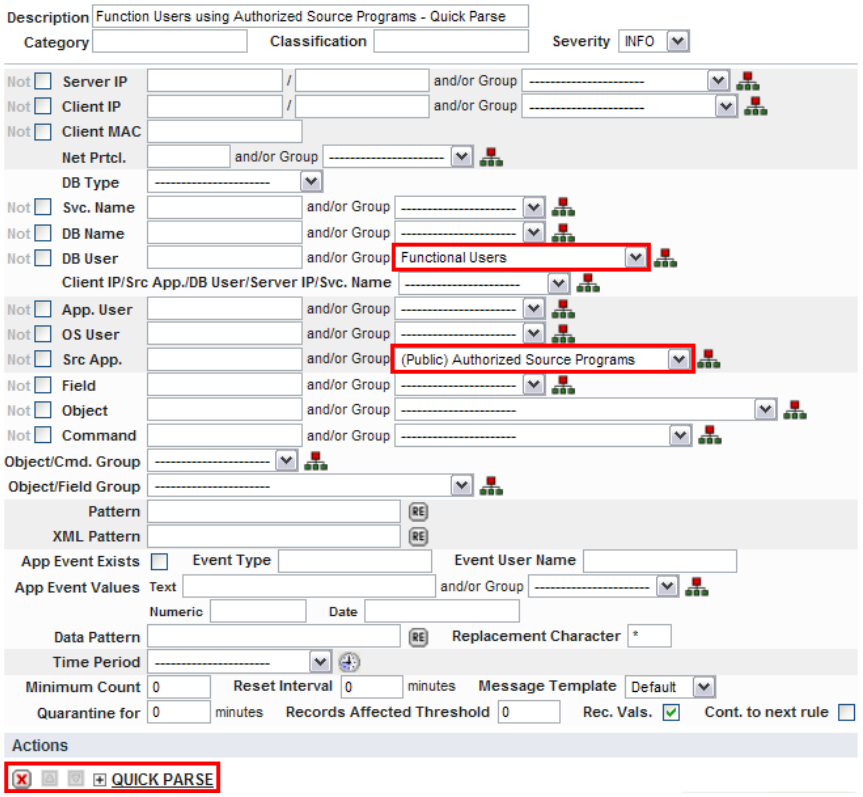
Figure 9-50. Log only GU2022.0

Notes:

The *Log Only* rule can be thought of as *Log (policy violation) Only*. It is similar to an alert in that any time the rule is trigged a policy violation will be created. This is useful when you need to report on specific policy violations but do not require an alert.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Quick parse



© Copyright IBM Corporation 2011, 2013

Figure 9-51. Quick parse GU2022.0

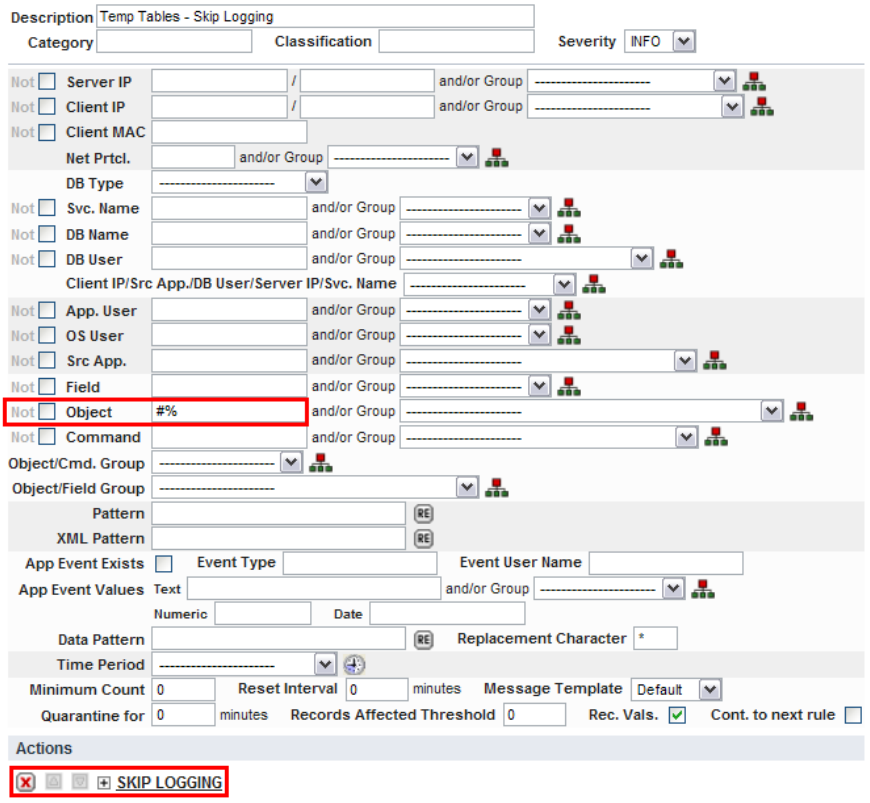
Notes:

When a **Quick Parse** rule is triggered for the remainder of the session, WHERE clauses will not be parsed. This reduces parsing time. In this mode, all objects accessed can be determined (since objects appear before the WHERE clause), but the exact object instances affected will be unknown, since that is determined by the WHERE clause.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Skip logging


Description Temp Tables - Skip Logging
Category
Classification
Severity INFO
Not Server IP / and/or Group
Not Client IP / and/or Group
Not Client MAC
Net Prtcl. and/or Group
DB Type
Not Svc. Name and/or Group
Not DB Name and/or Group
Not DB User and/or Group
Client IP/Src App./DB User/Server IP/Svc. Name
Not App. User and/or Group
Not OS User and/or Group
Not Src App. and/or Group
Not Field and/or Group
Not Object #% and/or Group
Not Command and/or Group
Object/Cmd. Group
Object/Field Group
Pattern
XML Pattern
App Event Exists Event Type Event User Name
App Event Values Text and/or Group
Numeric Date
Data Pattern Replacement Character *
Time Period
Minimum Count 0 Reset Interval 0 minutes Message Template Default
Quarantine for 0 minutes Records Affected Threshold 0 Rec. Vals. Cont. to next rule
Actions
SKIP LOGGING

© Copyright IBM Corporation 2011, 2013

Figure 9-52. Skip logging GU2022.0

Notes:

Skip Logging: When matched, do not log a policy violation, and stop logging constructs. This action is used to eliminate the logging of constructs for requests that are known to be of no interest. For example, this is commonly used with temp tables (object beginning with a pound sign (#)) in MS SQL Server.

This feature also applies for exception rules concerning database error code only, allowing users to not log errors when an application generates large amounts of errors and there is nothing that the user can do to stop the application errors.

These SQL requests or SQL errors are still sent by STAP and is still processed by the sniffer. It helps in data retention and eases reporting but does not provide the same performance benefit as ‘Ignore STAP Session’. It is only meant to be used when ignoring a small number of SQL requests. If you cannot use ‘Ignore STAP Session’ but would like to ignore many types of requests (for example, log DDL and DML but ignore everything else) a Selective Audit Trail policy would be more effective.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. True or false: The Action portion of a rule is executed whenever the conditions in the rule are met.

2. True or false: You can only have one action per rule.

3. True or false: Access rules are ANDed left to right and ORed row to row.

4. True or false: An ALERT logs information as well as sending out an email or some other kind of notification.

5. What is the effect of an Ignore Session action on an SQL statement?

6. What is the effect of a Log Full Details action on an SQL statement?

© Copyright IBM Corporation 2011, 2013

Figure 9-53. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

6.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. **True** or false: The Action portion of a rule is executed whenever the conditions in the rule are met.
2. True or **false**: You can only have one action per rule.
3. True or **false**: Access rules are ANDed left to right and ORed row to row.
4. True or **false**: An ALERT logs information as well as sending out an email or some other kind of notification.
5. What is the effect of an Ignore Session action on an SQL statement?
   The SQL is NOT sent on to the database server.
6. What is the effect of a Log Full Details action on an SQL statement?
   The entire SQL statement, including any values it contains, are logged.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Create and understand access rules

© Copyright IBM Corporation 2012, 2013

Figure 9-54. Topic summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. **True** or false: The Action portion of a rule is executed whenever the conditions in the rule are met.
2. True or **false**: You can only have one action per rule.
3. True or **false**: Access rules are ANDed left to right and ORed row to row.
4. True or **false**: An ALERT logs information as well as sending out an email or some other kind of notification.
5. What is the effect of an Ignore Session action on an SQL statement?
   The SQL is NOT sent on to the database server.
6. What is the effect of a Log Full Details action on an SQL statement?
   The entire SQL statement, including any values it contains, are logged.

© Copyright IBM Corporation 2011, 2013

Figure 9-55. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

9.4. Exception and Extrusion Rules

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exception and Extrusion rules

After completing this topic, you should be able to:

- Create exception rules within a policy
- Create a *failed logins* alert
- Enable extrusions rules
- Create an extrusion rule

© Copyright IBM Corporation 2012, 2013

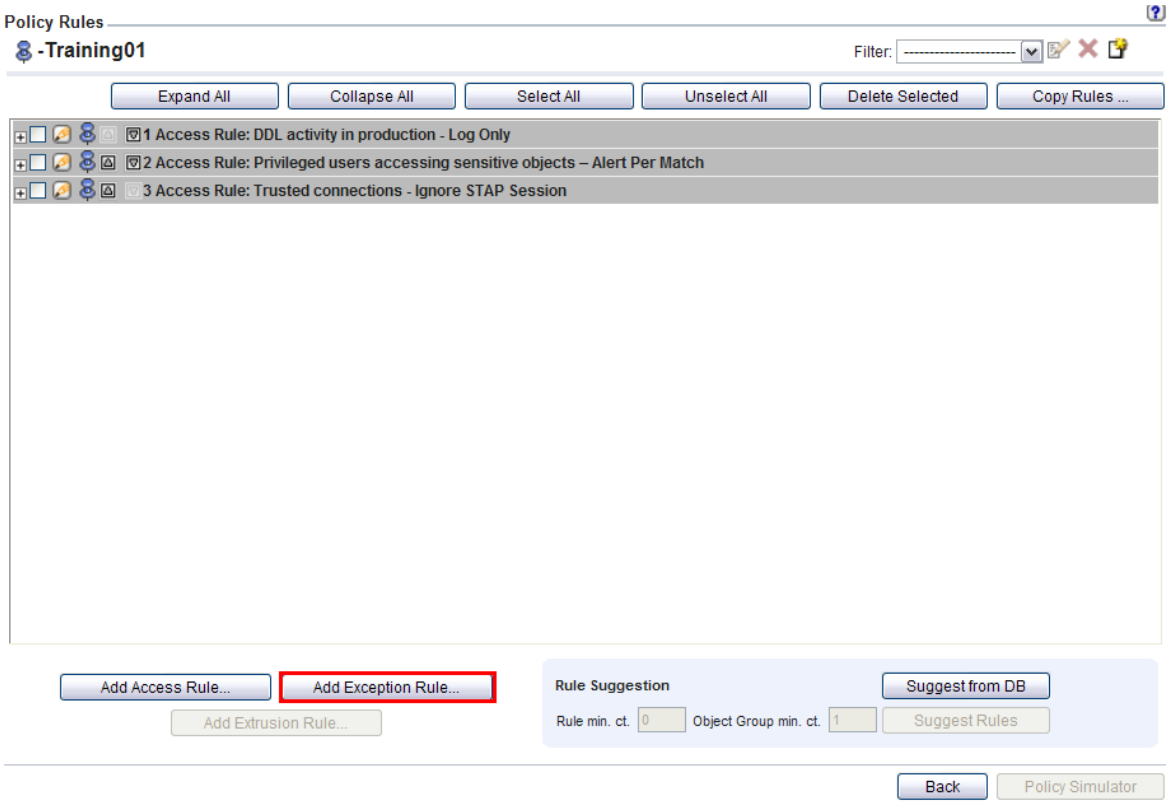
Figure 9-56. Exception and Extrusion rules GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exception Rule overview



© Copyright IBM Corporation 2011, 2013

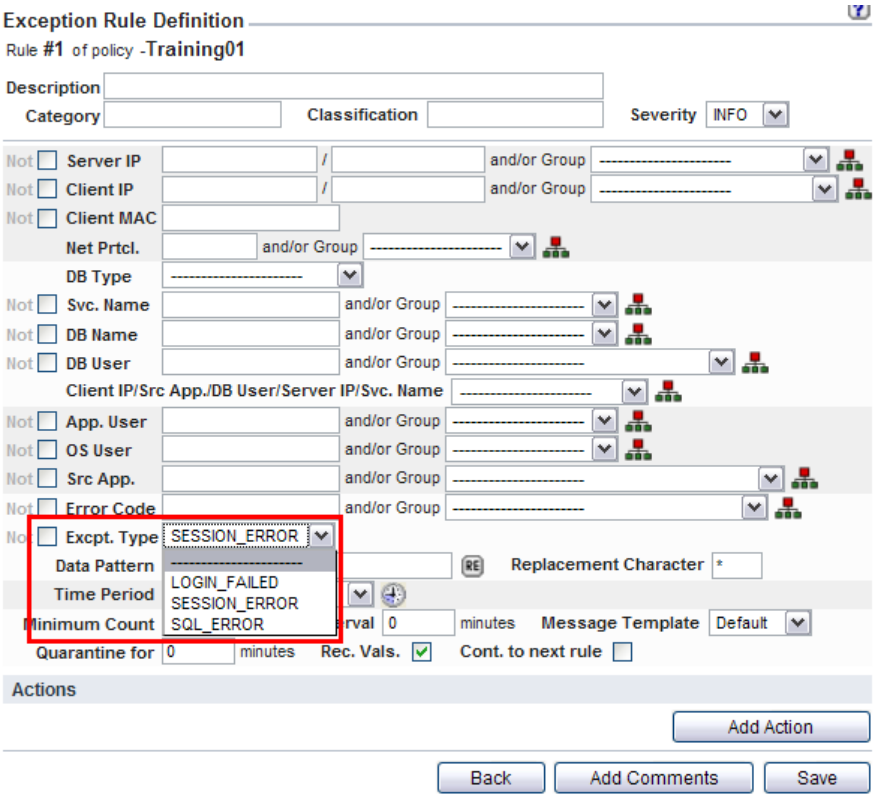
Figure 9-57. Exception Rule overview GU2022.0

Notes:

Exception rules evaluate exceptions returned by the database server to the client, generally failed logins and SQL errors.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exception Rule Definition



© Copyright IBM Corporation 2011, 2013

Figure 9-58. Exception Rule Definition GU2022.0

Notes:

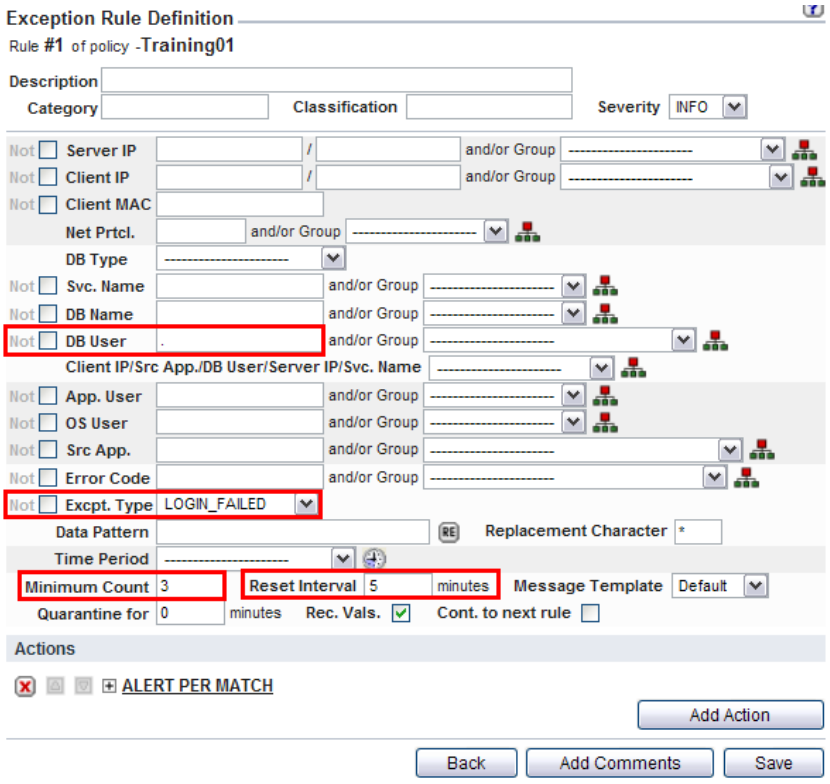
Exception rules contain session-level criteria, like access rules, but do not have criteria for SQL request (command, object, etc.). Instead, Exception rules contain a field for **Exception Type**, which includes:

- **LOGIN_FAILED -** failed login messages from the database server to the database client
- **SESSION_ERROR** - errors related to connection information
- **SQL_ERROR** - error messages returned from the database server to the database client. For example, when executing select against a table that does not exist in DB2 will return this error: *SQL0204N "A8000.TABLC" is an undefined name. SQLSTATE=42704*

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Failed login alert



© Copyright IBM Corporation 2011, 2013

Figure 9-59. Failed login alert GU2022.0

Notes:

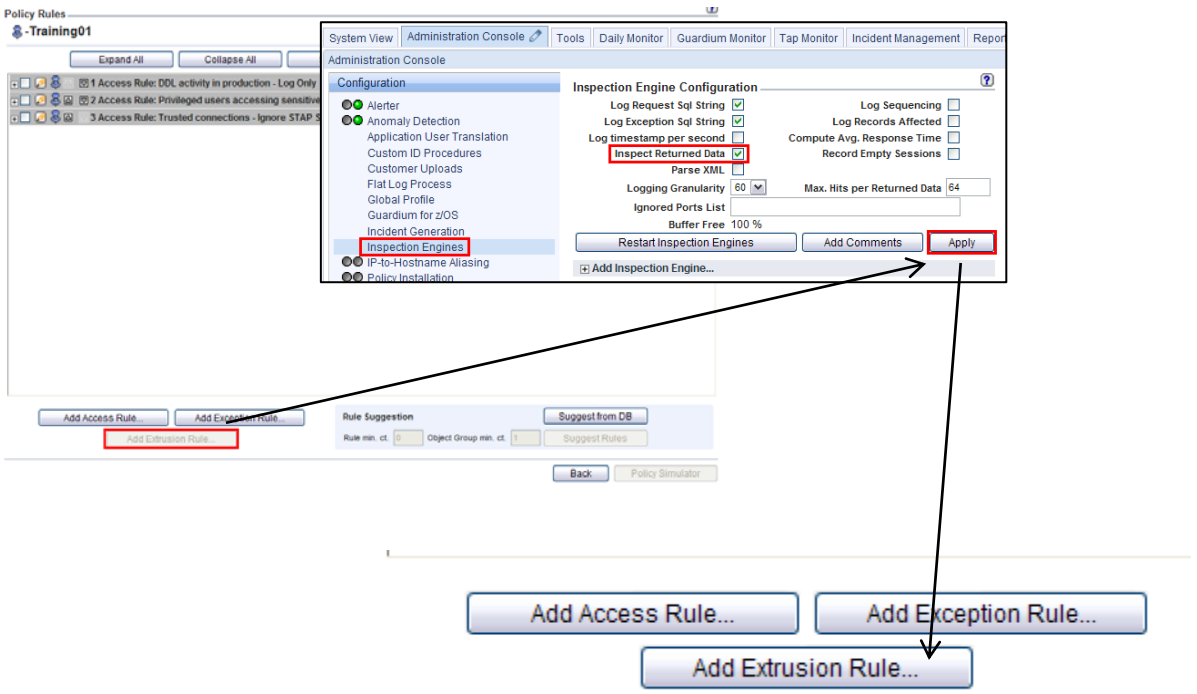
The most common type of exception rule created is to alert on *x* number of failed login attempts within *x* minutes; for example 3 failed login attempts within 5 minutes.

To create this alert, create a new exception rule as follows:

- **Action** = *Alert Per Match*
- **Minimum Count** = 3
- **Reset Interval** = 5
- **Excpt. Type** = LOGIN_FAILED
- **DB User** = . <period>. Placing a period in DB User causes to the system to place a counter on DB User, so that you will only receive an alert the same user attempts to login three times with in five minutes. Otherwise, it will alert whenever there are three failed logins from any three users within five minutes, which could result in a great deal of false positives.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Extrusion Rules



© Copyright IBM Corporation 2011, 2013

Figure 9-60. Extrusion Rules GU2022.0

Notes:

An **extrusion rule** evaluates data returned by the server (in response to requests) - for example, it might test the returned data for numeric patterns that could be social security or credit card numbers.

Before using extrusion rules, they must be enabled as follows:

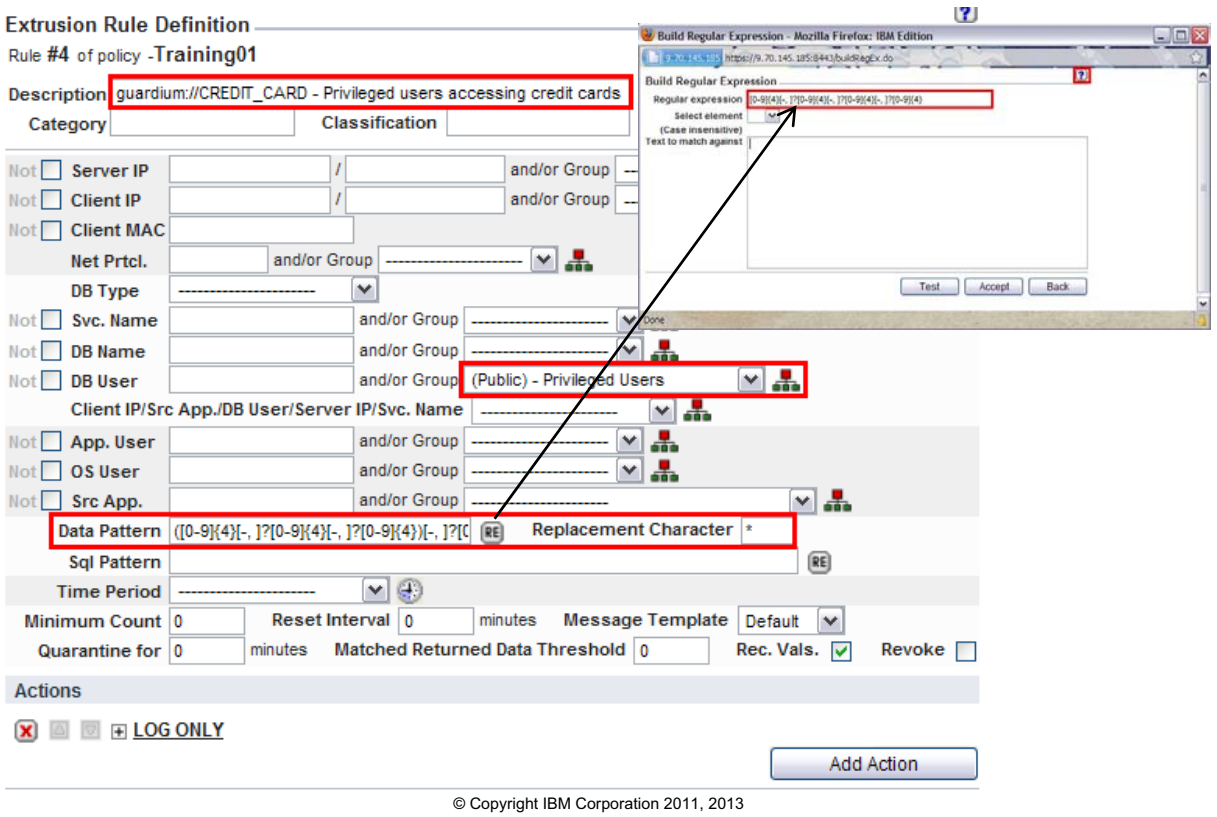
- Go to **Administration Console** -> **Inspection Engines**
- Check the **Inspect Returned Data** checkbox
- Press **Apply**

After making this change, you will see that the **Add Extrusion Rule** button will no longer be grayed out.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Extrusion Rule example



© Copyright IBM Corporation 2011, 2013

Figure 9-61. Extrusion Rule example GU2022.0

Notes:

Extrusion rules examine data being returned from the database server to the client based on patterns in the data, matching a Regular Expression.

To create an extrusion rule, searching for credit card numbers being returned to privileged users, populate the fields as follows:

- **Description** – *guardium://CREDIT_CARD – Privileged users accessing credit cards*
  - When a rule name begins with "guardium://CREDIT_CARD", and there is a valid credit card number pattern in the Data pattern field, the policy will use the Luhn algorithm (a widely-used algorithm for validating identification numbers such as credit card numbers), in addition to standard pattern matching. The Luhn algorithm is an additional check and does not replace the pattern check. A valid credit card number is a string of 16 digits or four sets of four digits, with each set separated by a blank. There is a requirement to have both the guardium://CREDIT_CARD rule name and a valid [0-9]{16} number in the Search Expression box in order to have the Luhn algorithm involved in this pattern matching.

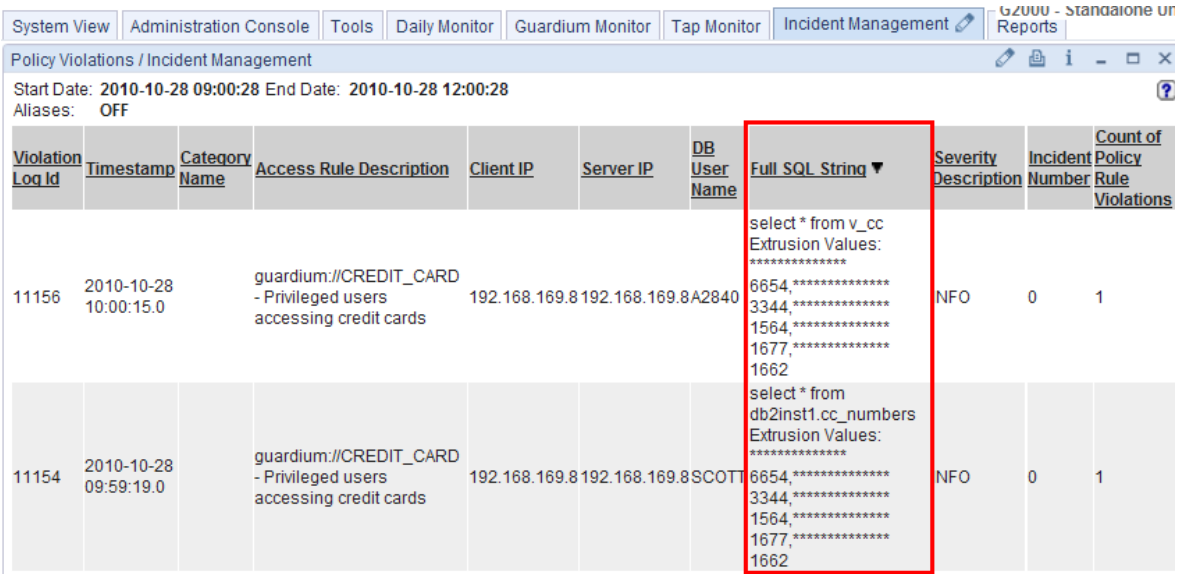
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **DB User** IN GROUP *Privileged Users*
- **Data Pattern** - ([0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}**)**[-,]?[0-9]{4}
    - This is a regular expression that will search for any string of 16 digits or four sets of four digits, with each set separated by a blank or a dash.
    - The parenthesis are surrounding the portion of the string that will be masked when logged by Guardium. In this case, only the last 4 digits of the credit card numbers will be logged.
    - To receive help in building a regular expression, press the 'RE' button, which will bring up the *Build Regular Expression* box where you can test your regular expression. Press the question mark (?) button will provide a help page with example regular expression to cover many types of date (credit card numbers, social security numbers, etc)
- **Replacement Character** – if you would like to use something other than as asterisk to mask the string, enter it here.
- **Action** – extrusion rules can write to the policy violations domain through Alert or Log Only rules or to the access domain through Log Full Details rules. In the example above, it will write to the policy violation domain, which is visible on the Incident Management tab.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Extrusion rule results example



© Copyright IBM Corporation 2011, 2013

Figure 9-62. Extrusion rule results example GU2022.0

Notes:

This example shows how Guardium logs and displays the data resulting from an extrusion rule firing. The Full SQL string contains the SQL string that was issued and the masked values that the database server returned.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. Explain why you might need to put a period (.) in the DBUser field when setting up a failed login exception rule.
2. True or false: An exclusion rule can be created to detect and log information on SQL error messages that are generated.
3. Explain what a “regular expression” is.
4. To have Guardium examine an actual result set value during an extrusion rule’s evaluation, the _____ option box must be selected.
5. Which character is used by default when masking a value with an extrusion rule?
   a. *
   b. ?
   c. <blank>
   d. -

© Copyright IBM Corporation 2011, 2013

Figure 9-63. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. Explain why you might need to put a period (.) in the DBUser field when setting up a failed login exception rule.

   Without the period, Guardium will check the number of failed logins in a given time period *for all users.* **With the period, Guardium will check the number of failed logins in a given time period** *for each user.*

2. **True** or false: An exclusion rule can be created to detect and log information on SQL error messages that are generated.

3. Explain what a regular expression is.

   A regular expression is a set of data pattern characters.

4. To have Guardium examine an actual result set value during an extrusion rules evaluation, the **Inspect Returned Data** option box must be selected.

5. Which character is used by default when masking a value with an extrusion rule?

   a. *

   b. ?

   c. <blank>

   d. -

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Create exception rules within a policy
- Create a *failed logins* alert
- Enable extrusions rules
- Create an extrusion rule

© Copyright IBM Corporation 2011, 2013

Figure 9-64. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. Explain why you might need to put a period (.) in the DBUser field when setting up a failed login exception rule. **Without the period, Guardium will check the number of failed logins in a given time period *for all users.* With the period, Guardium will check the number of failed logins in a given time period *for each user.***

2. **True** or false: An exclusion rule can be created to detect and log information on SQL error messages that are generated.

3. Explain what a “regular expression” is. **A regular expression is a set of data pattern characters.**

© Copyright IBM Corporation 2011, 2013

Figure 9-65. Checkpoint solutions GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions continued

4. To have Guardium examine an actual result set value during an extrusion rule's evaluation, the **Inspect Returned Data** option box must be selected.
5. Which character is used by default when masking a value with an extrusion rule?
   a. *
   b. ?
   c. <blank>
   d. -

© Copyright IBM Corporation 2011, 2013

Figure 9-66. Checkpoint solutions continued GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

9.5. Selective Audit Trail policy

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Selective Audit Trail policy

After completing this topic, you should be able to:

- Understand the Selective Audit Trail policy
- Create an *Audit Only* policy rule

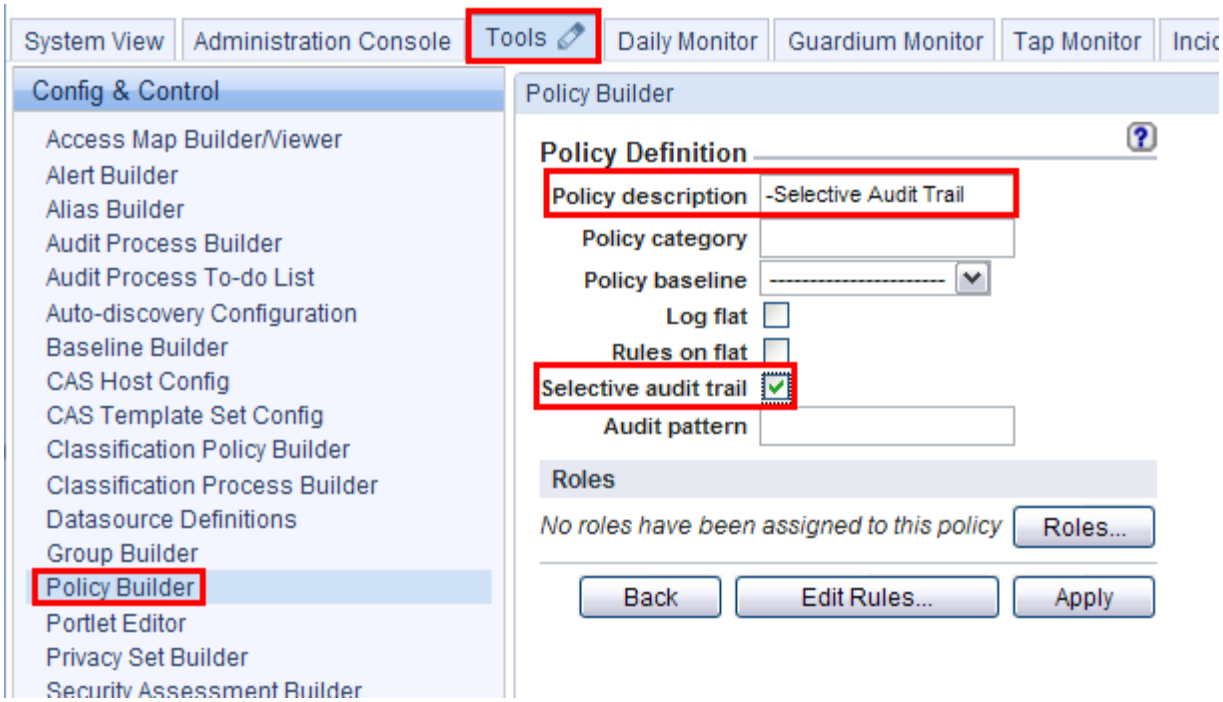
© Copyright IBM Corporation 2011, 2013

Figure 9-67. Selective Audit Trail policy GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Creating a Selective Audit Trail policy



© Copyright IBM Corporation 2011, 2013

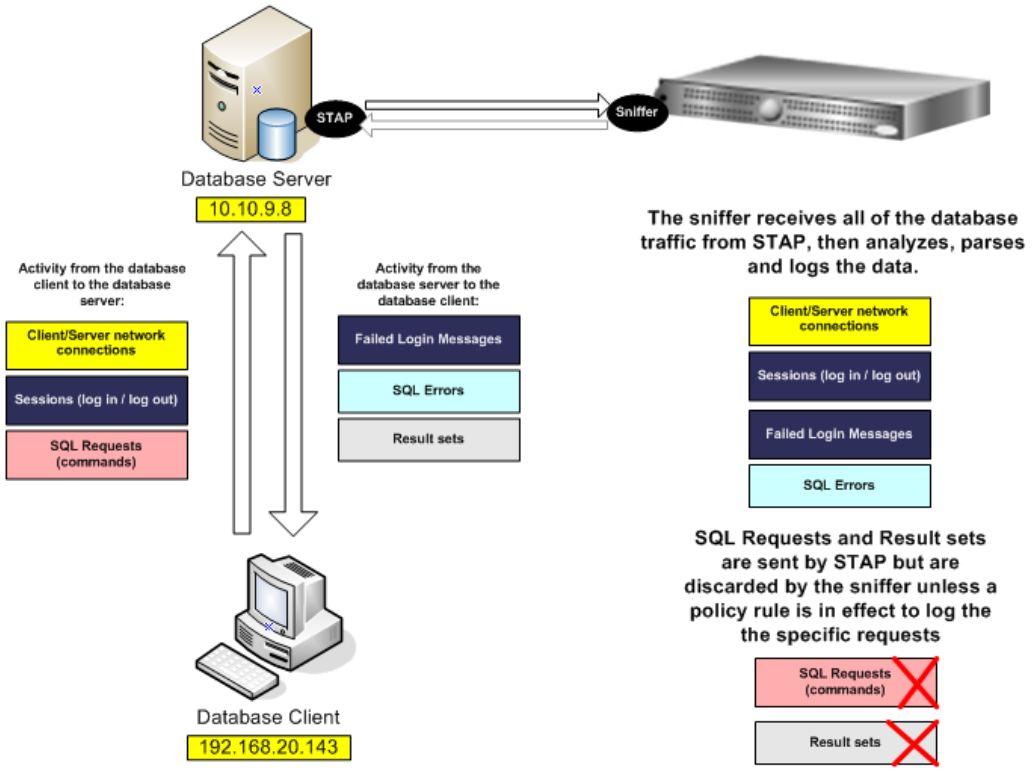
Figure 9-68. Creating a Selective Audit Trail policy GU2022.0

Notes:

Some implementations require that only a small subset of SQL requests be monitored; for example, *sensitive object access* only or *DML and DDL activity* only. In these situations, a Selective Audit Trail policy can provide tremendous benefits both in collector performance and data retention.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Selective Audit Trail default behavior


STAP
Sniffer
Database Server
10.10.9.8
Activity from the database client to the database server:
Client/Server network connections
Sessions (log in / log out)
SQL Requests (commands)
Activity from the database server to the database client:
Failed Login Messages
SQL Errors
Result sets
The sniffer receives all of the database traffic from STAP, then analyzes, parses and logs the data.
Client/Server network connections
Sessions (log in / log out)
Failed Login Messages
SQL Errors
SQL Requests and Result sets are sent by STAP but are discarded by the sniffer unless a policy rule is in effect to log the the specific requests
SQL Requests (commands)
Result sets
Database Client
192.168.20.143

© Copyright IBM Corporation 2011, 2013

Figure 9-69. Selective Audit Trail default behavior GU2022.0

Notes:

This slide describes the default behavior if you were to install a selective audit policy with no rules.

Traffic sent by STAP

Database Client -> Database Server

- Client/server network connections
- Sessions (logins/logouts)
- SQL requests (commands)

Database Server-> Database Client

- Failed login messages
- SQL errors
- Result sets

Traffic analyzed, parsed and logged by the sniffer

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Database Client -> Database Server

- Client/server network connections
- Sessions (logins/logouts)

Database Server-> Database Client

- Failed login messages
- SQL errors

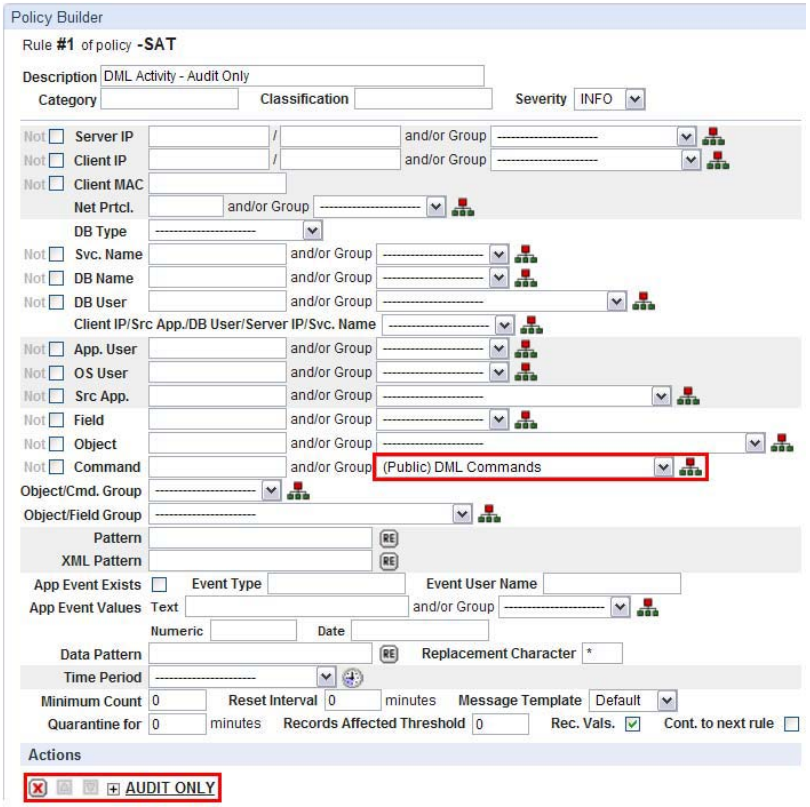
Traffic ignored and discarded by the sniffer

- SQL Requests*
- Result sets

* The policy must contain a rule to log specific SQL requests, otherwise they will be discarded. Alternately, you may enter a regular expression in the *Audit Pattern* field. However, this is not commonly used.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Audit Only rule



© Copyright IBM Corporation 2011, 2013

Figure 9-70. Audit Only rule GU2022.0

Notes:

When an *Audit Only* rule fires in a selective audit trail policy, the appliance will log the traffic normally (constructs with masked SQL and the Access Period timestamp). If you need to log the full SQL string, Log Full Details rules will work the same as in a non-selective audit trail policy. Also, ignore session rules can be used in a selective audit and still provide tremendous performance benefits.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. Explain what a selective audit trail policy is.

© Copyright IBM Corporation 2011, 2013

Figure 9-71. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. Explain what a selective audit trail policy is.

   A selective audit trail policy is a method of filtering which SQL requests will be monitored.

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Understand the Selective Audit Trail policy
- Create an *Audit Only* policy rule

© Copyright IBM Corporation 2011, 2013

Figure 9-72. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solution

1. Explain what a selective audit trail policy is. **A selective audit trail policy is a method of filtering which SQL requests will be monitored.**

© Copyright IBM Corporation 2011, 2013

Figure 9-73. Checkpoint solution GU2022.0

Notes:

Write your answers here:

1.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

9.6. Rule Order and Logic

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Rule order and logic

After completing this topic, you should be able to:

- Order policy rules so that actions are triggered properly

© Copyright IBM Corporation 2011, 2013

Figure 9-74. Rule order and logic GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Rule order and policy logic

- Rule order can affect whether policy rules fire correctly or not
- Actions and settings that can affect the policy logic include:
  - Multiple actions
  - Continue to next rule
  - Ignore session rules
  - Exception versus access rules

© Copyright IBM Corporation 2011, 2013

Figure 9-75. Rule order and policy logic GU2022.0

Notes:

This slide describes the default behavior if you were to install a selective audit policy with no rules.

- **Multiple actions** – if you require two actions for the same criteria, use multiple actions
  - Example, *Alert Per Match* AND *Log Masked Details* for DML on Sensitive Objects.
- **Continue to Next Rule** – if you have two requirements which do not have the same criteria but do have some overlap, use the **Cont. to next rule** checkbox.
- **Ignore session rules** – In general, ignore session rules should be the first access rules
  - An Exception to this rule of thumb would be a ‘catch-all’ rule at the end of your policy that ignores all sessions that did not match the previous. Also, as described on the “Allow” slide, sometimes you may need to temporarily prevent an ignore session rule from being fired by placing it after an “allow” rule.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

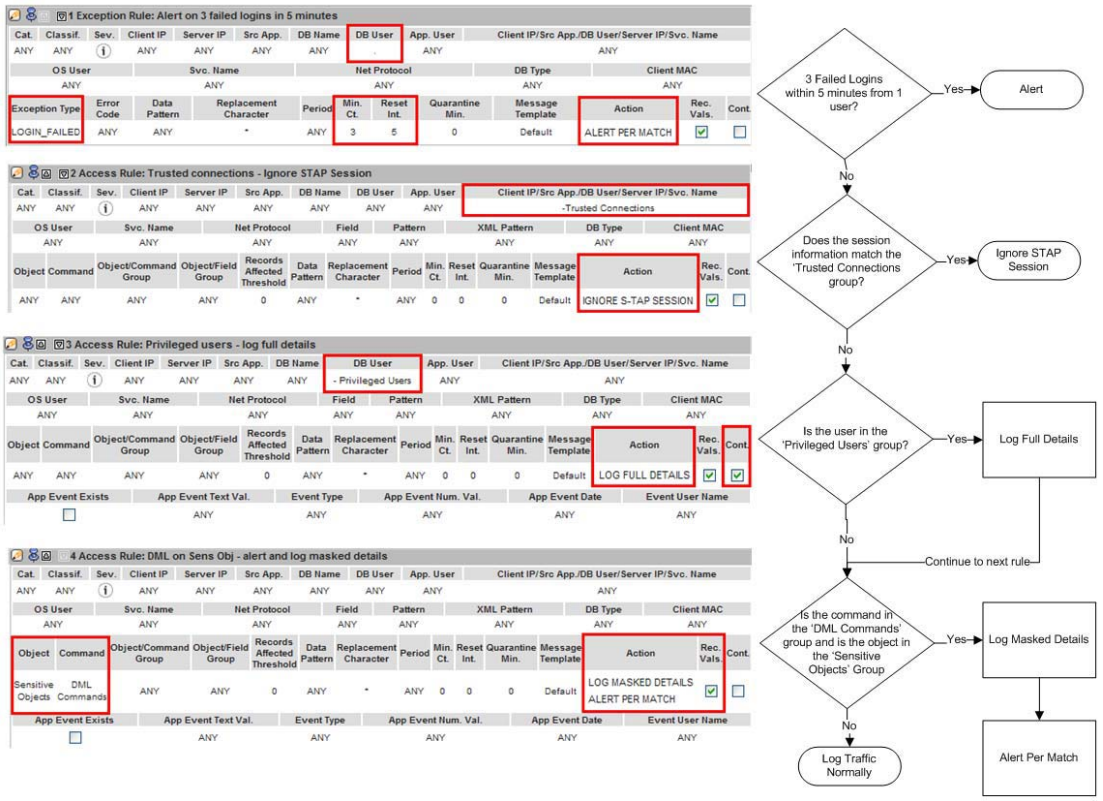
  - Remember, once a session is ignored, no activity within that session will be processed.

- **Exceptions and Access rules** – Exceptions and access rules are generally mutually exclusive because they are examining different sides of the traffic flow. Usually, these rules types do not have much affect on each other.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Policy logic


1 Exception Rule: Alert on 3 failed logins in 5 minutes
2 Access Rule: Trusted connections - Ignore STAP Session
3 Access Rule: Privileged users - log full details
4 Access Rule: DML on Sens Obj - alert and log masked details
3 Failed Logins within 5 minutes from 1 user?
Yes
Alert
No
Does the session information match the 'Trusted Connections group?
Yes
Ignore STAP Session
No
Is the user in the 'Privileged Users' group?
Yes
Log Full Details
No
Continue to next rule
Is the command in the 'DML Commands' group and is the object in the 'Sensitive Objects' Group
Yes
Log Masked Details
No
Log Traffic Normally
Alert Per Match

© Copyright IBM Corporation 2011, 2013

Figure 9-76. Policy logic GU2022.0

Notes:

In the example above, the incoming database traffic will be evaluated as follows:

- Have there been 3 failed logins with in 5 minutes from a singe user? If yes, *alert*. If not go to the next rule.
  - Note, because this rule is an exception rule and the remaining rules are access rules, this rule could have been placed anywhere.
- Does the session information match the ‘Trusted Connection’ group? If yes, *Ignore STAP Session*. If no, go to the next rule.
  - This should be the first access rule because all of the trusted connections should be ignored. If placed lower in the rule order, some rules may fire inappropriately.
- Is the user in the ‘Privileged User’ group? If yes, *Log Full Details* and *Continue to next rule*

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

  - If the *Cont*. box is not checked, the policy would stop at this rule for all privileged user activity. So, in order to ensure that rule number 4 is processed for privileged users, you must check the *Cont.* box.

- Is the object in the 'Sensitive Objects' group and is the command in the 'DML Commands' group? If yes, *Log Masked Details* and *Alert Per Match*.
  - If the user is a privileged user, the *Log Full Details* action from rule number 3 will take precedence.
- If none of the above are matched, then log traffic normally.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Checkpoint

1. True or false: The order in which rules are recorded in a policy is not important.

2. Which option box must be checked to force evaluation of the next rule when the current rule is evaluated as true?
   a. NEXT
   b. CONT
   c. MORE
   d. GOTO

3. Explain what happens if none of the rules in a policy are evaluated as true.

© Copyright IBM Corporation 2011, 2013

Figure 9-77. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. True or **false**: The order in which rules are recorded in a policy is not important.
2. Which option box must be checked to force evaluation of the next rule when the current rule is evaluated as true?
   a. NEXT
   b. CONT
   c. MORE
   d. GOTO
3. Explain what happens if none of the rules in a policy are evaluated as true.

   The incoming message is passed to the database server as usual for evaluation and execution.

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Topic summary

After completing this topic, you should be able to:

- Order policy rules so that actions are triggered properly

© Copyright IBM Corporation 2011, 2013

Figure 9-78. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. True or **false**: The order in which rules are recorded in a policy is not important.

2. Which option box must be checked to force evaluation of the next rule when the current rule is evaluated as true?
   a. NEXT
   b. CONT
   c. MORE
   d. GOTO

3. Explain what happens if none of the rules in a policy are evaluated as true. **The incoming message is passed to the database server as usual for evaluation and execution.**

© Copyright IBM Corporation 2011, 2013

Figure 9-79. Checkpoint solutions GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 7** in the Exercise Guide. Alternately, you can wait and do Exercises 6 and 7 at the end of this unit.

© Copyright IBM Corporation 2011, 2013

Figure 9-80. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

9.7. S-GATE

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-GATE

After completing this topic, you should be able to:

- Describe the use of S-GATE

© Copyright IBM Corporation 2011, 2013

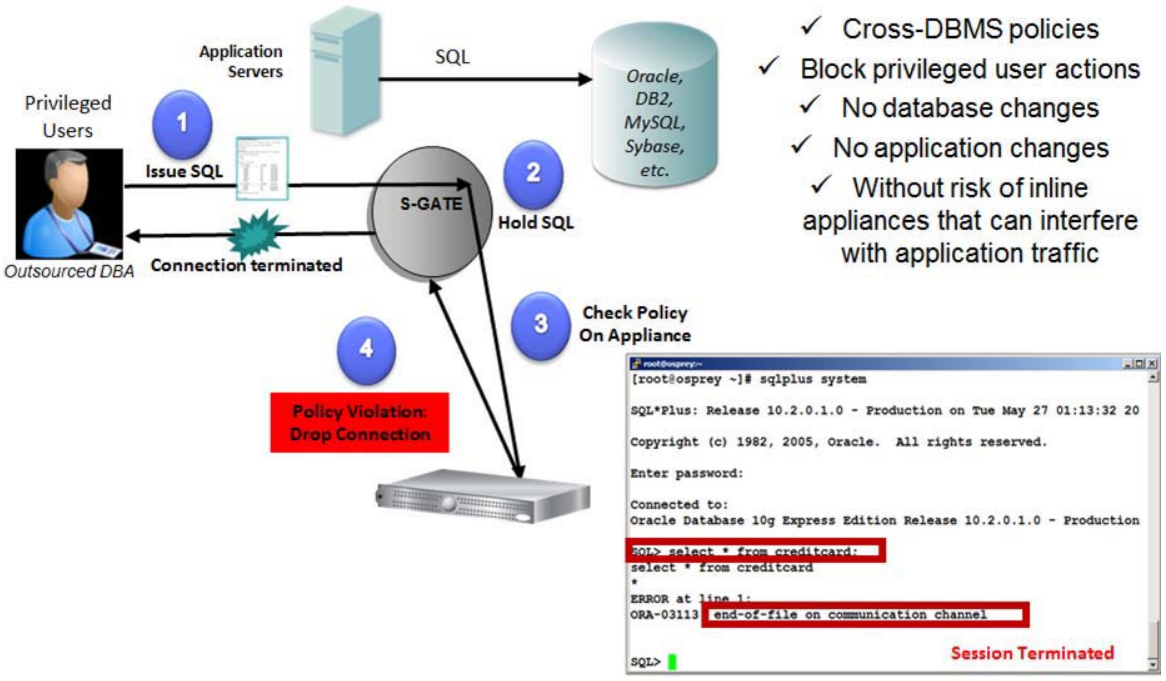
Figure 9-81. S-GATE GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-GATE overview



© Copyright IBM Corporation 2011, 2013

Figure 9-82. S-GATE overview GU2022.0

Notes:

In addition to monitoring, S-TAP can also be configured to work in firewall mode.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-GATE S-TAP settings

```
dbserver01:~ # cat /usr/guardium/modules/STAP/8.1.0
0_r24276_1-1298065578/guard_tap.ini |grep firewall
firewall_default_state=0
firewall_fail_close=0
firewall_installed=1
firewall_timeout=10
```

© Copyright IBM Corporation 2011, 2013

Figure 9-83. S-GATE S-TAP settings GU2022.0

Notes:

S-GATE must be enabled from S-TAP before using S-GATE rules.

- **firewall_installed** = should the firewall feature be enabled at all
  - 0=No,1=Yes (0)
- **firewall_fail_close** = what is the default action when verdict can not be set by the policy rules (e.g. timeout reached)
  - 0=let connection through
  - 1=block connection (0)
- **firewall_default_state =** What triggers the start of the firewall mode
  - 0=event triggering a rule in the installed policy happens
  - 1=start in firewall mode enabled regardless of a triggering event (0)

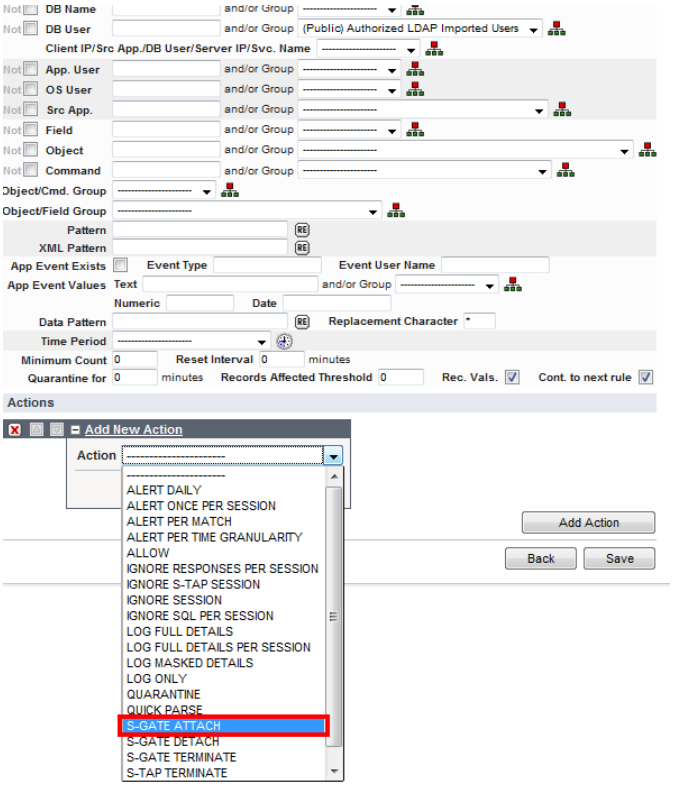
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **firewall_timeout** = time (in seconds) to wait on a verdict from the appliance if timed out look at firewall_fail_close value to know whether to block or allow the connection (10 seconds)

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-GATE ATTACH/DETACH



© Copyright IBM Corporation 2011, 2013

Figure 9-84. S-GATE ATTACH/DETACH GU2022.0

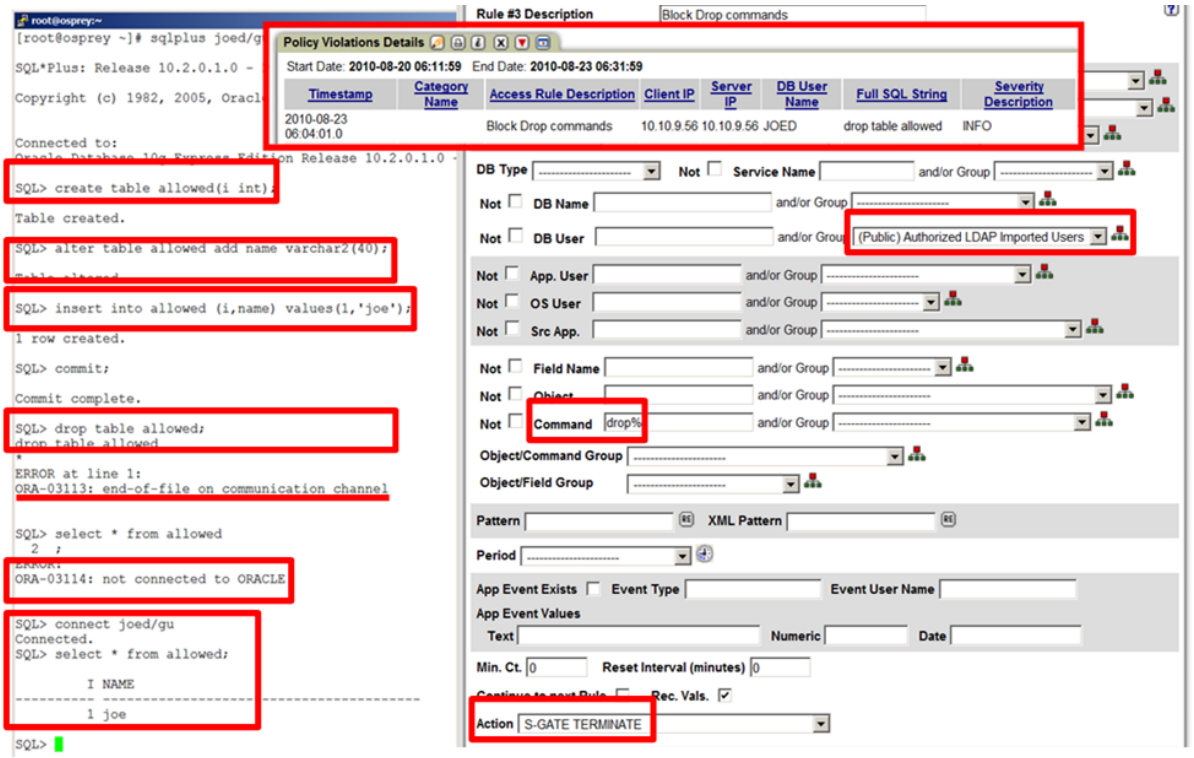
Notes:

Before a user can be terminated the user must be in firewall mode. If the firewall_default_state is set to 0, to put the user in firewall mode you must apply the rule **S-GATE ATTACH** (this should be fore privileged users only). If the firewall_default_state =1, then all users will be attached by default. This can cause some latency, so applications should never be left in firewall mode. In this case use **S-GATE DETACH** to take applications out of firewall mode.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

S-GATE Terminate



© Copyright IBM Corporation 2011, 2013

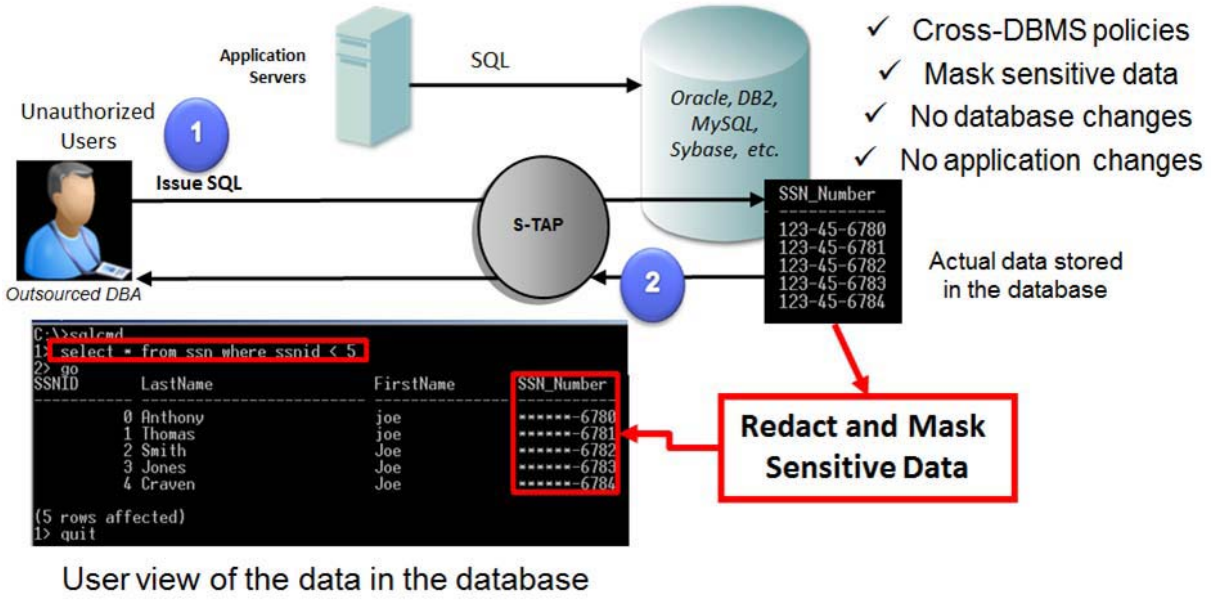
Figure 9-85. S-GATE Terminate GU2022.0

Notes:

The S-GATE terminate action will block the SQL command from reaching the database server and drop the user's session.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Redact



© Copyright IBM Corporation 2011, 2013

Figure 9-86. Redact GU2022.0

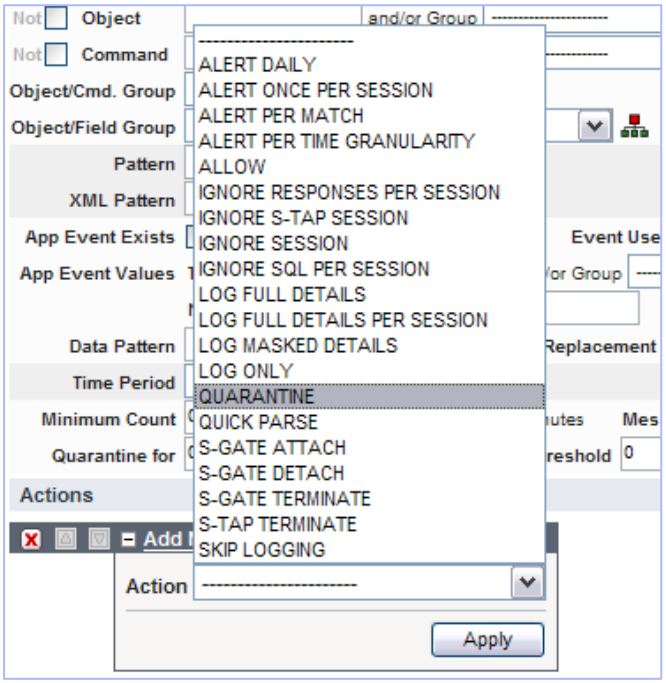
Notes:

For extrusion rules only, redact masks sensitive data returned to the user from the database server.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Quarantine



© Copyright IBM Corporation 2011, 2013

Figure 9-87. Quarantine GU2022.0

Notes:

The QUARANTINE action will quarantine a user access until specified date.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

After completing this topic, you should be able to:

- Describe the use of S-GATE

© Copyright IBM Corporation 2011, 2013

Figure 9-88. Topic summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. Explain the purpose of S-GATE.

2. Which S-GATE option is utilized to put a user in firewall mode?
   a. S-GATE ATTACH
   b. S-GATE FIREWALL
   c. S-GATE JOIN
   d. S-GATE BEGIN

3. Explain what REDACTion does.

4. What happens to a user's session when it is S-GATE TERMinated?

© Copyright IBM Corporation 2011, 2013

Figure 9-89. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. Explain the purpose of S-GATE.

   S-GATE acts proactively as a firewall, examining incoming messages before they reach the database server.

2. Which S-GATE option is utilized to put a user in firewall mode?

   a. **S-GATE ATTACH**

   b. S-GATE FIREWALL

   c. S-GATE JOIN

   d. S-GATE BEGIN

3. Explain what REDACTion does.

   Redaction marks out or masks all or part of a result set value.

4. What happens to a user's session when it is S-GATE TERMinated?

   The user's session is dropped (or disconnected) from the database server.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand how InfoSphere Guardium logs traffic
- Create a policy or set of policies to meet your requirements
- Install and manage policies
- Note: The following topics will not be covered during this training:
  - Baselines
  - Flat logging

© Copyright IBM Corporation 2011, 2013

Figure 9-90. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- If you waited to do exercises, you should complete **Exercises 6 and 7** in the Exercise Guide at this point.

© Copyright IBM Corporation 2012, 2013

Figure 9-91. Exercise GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. Explain the purpose of S-GATE. **S-GATE acts proactively as a firewall, examining incoming messages before they reach the database server.**

2. Which S-GATE option is utilized to put a user in firewall mode?
   a. **S-GATE ATTACH**
   b. S-GATE FIREWALL
   c. S-GATE JOIN
   d. S-GATE BEGIN

3. Explain what REDACTion does. **Redaction marks out or masks all or part of a result set value.**

4. What happens to a user's session when it is S-GATE TERMinated? **The user's session is dropped (or disconnected) from the database server.**

© Copyright IBM Corporation 2011, 2013

Figure 9-92. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Unit 10. CAS, VA, and Discovery

Estimated time

00:30

What this unit is about

This unit describes the components of the Configuration Auditing System and explains the value of Vulnerability Assessment.

What you should be able to do

After completing this unit, you should be able to:

- Understand the major components of the Configuration Auditing System (CAS)
- Understand the value of Vulnerability Assessment
- Understand why Database Discovery is needed

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand the major components of the Configuration Auditing System (CAS)
- Understand the value of Vulnerability Assessment
- Understand why Database Discovery is needed

© Copyright IBM Corporation 2011, 2013

Figure 10-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CAS

The Configuration Auditing System

- Defines and runs tests at the operating system level on the database server
- Compares results against predefined and expected values
- Checks items including:
  - Database configurations
  - File permissions
  - Directory existence
  - Etc

© Copyright IBM Corporation 2011, 2013

Figure 10-2. CAS GU2022.0

Notes:

Configuration Auditing System (CAS)

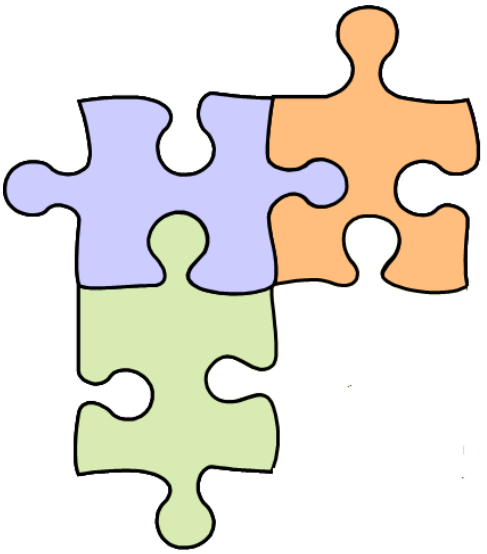
Databases can be affected by changes to the server environment; for example, by changing configuration files, environment or registry variables, or other database or operating system components, including executables or scripts used by the database management system or the operating system. CAS tracks such changes and reports on them. The data is available on the Guardium appliance and can be used for reports and alerts.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

CAS Components

Configuration Auditing System (CAS)

- CAS includes:
  - **CAS Agent**
  - **CAS Server Authentication**
  - **Template Sets**



© Copyright IBM Corporation 2011, 2013

Figure 10-3. CAS Components GU2022.0

Notes:

Configuration Auditing System (CAS)

Databases can be affected by changes to the server environment; for example, by changing configuration files, environment or registry variables, or other database or operating system components, including executables or scripts used by the database management system or the operating system. CAS tracks such changes and reports on them. The data is available on the Guardium appliance and can be used for reports and alerts.

CAS Agent

CAS is an agent installed on the database server and reports to the Guardium appliance whenever a monitored entity is changed, either in content, ownership or permissions. You install a CAS client on the database server system, using the same utility that is used to install S-TAP. CAS shares configuration information with S-TAP, though each component runs independently of the other. Once the CAS client has been installed on the host, you configure the actual change auditing functions from the Guardium portal.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Template Set

A CAS template set contains a list of item templates, bundled together, share a common purpose such as monitoring a particular type of database (Oracle on Unix, for example), and is one of two types:

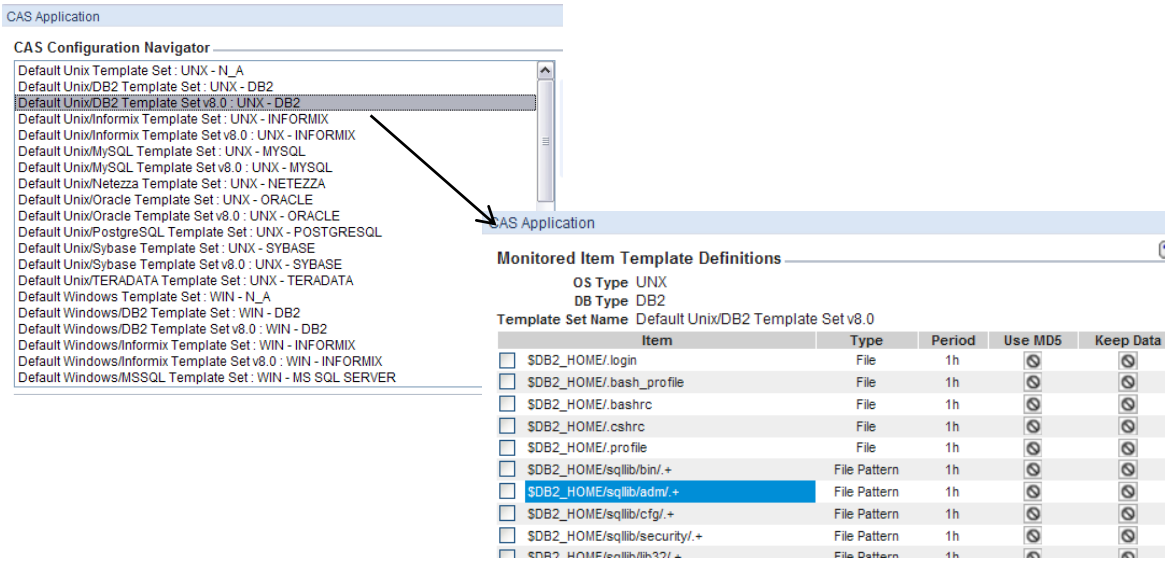
- Operating System Only (Unix or Windows)
- Database (Unix-Oracle, Windows-Oracle, Unix-DB2, Windows-DB2, etc.)

A database template set is always specific to both the database type and the operating system type.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration Auditing System (1 of 3)

- **Configuration Auditing System (CAS):**
  - **CAS Configuration**
  - **Default Template Sets**
  - **Database Templates**



© Copyright IBM Corporation 2011, 2013

Figure 10-4. Configuration Auditing System (1 of 3) GU2022.0

Notes:

CAS Configuration

A CAS configuration defines one or more CAS instances, each of which identifies a template set to be used to monitor a set of items on that host.

Default Template Sets

For each operating system and database type supported, Guardium provides a preconfigured, default template sets for monitoring a variety of databases on either Unix or Windows platforms. A default template set is one that will be used as a starting point for any new template set defined for that template-set type. A template-set type is either an operating system alone (Unix or Windows), or a database management system (DB2, Informix, Oracle, etc.), which is always qualified by an operating system type - for example, UNIX-Oracle, or Windows-Oracle. Many of the preconfigured, default template sets are used within Guardium's Vulnerability Assessments where, for example, known parameters, file locations, and file permissions can be checked.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The Guardium default template sets all begin with the word Guardium. You cannot modify a Guardium default template set, but you can clone it and modify the cloned version. Each of the Guardium default template sets defines a set of items to be monitored. Make sure that you understand the function and use of each of the items monitored by that default template set and use the ones that are relevant to your environment. After defining a template set of your own, you can designate that template set as the default template set for that template-set type. After that, any new template sets defined for that operating system and database type will be defined using your new default template set as a starting point. The Guardium default template set for that type will not be removed; it will remain defined, but will not be marked as the default.

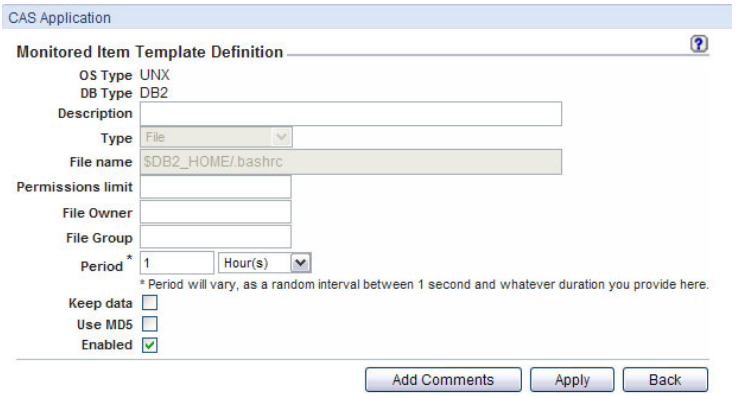
Database Templates

Each database has a set of defined CAS templates.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration Auditing System (2 of 3)

- **Configuration Auditing System (CAS):**
  - **CAS Template Item**
  - **Monitored Entity**
  - **CAS Instance**



© Copyright IBM Corporation 2011, 2013

Figure 10-5. Configuration Auditing System (2 of 3) GU2022.0

Notes:

CAS Template Item

The definition or set of attributes of a monitoring task over a single Monitored Entity. Users can define new CAS test to construct new CAS templates or use predefined templates for each OS and each database type; optionally modifying to meet specific database monitoring requirements.

A template item is a specific file or file pattern, an environment or registry variable, the output of an OS or SQL script, or the list of logged-in users. The state of any of these items is reflected by raw data, i.e. the contents of a file or the value of a registry variable. CAS detects changes by checking the size of the raw data, or computing a checksum of the raw data. For files, CAS can also check for system level changes such as ownership, access permission, and path for a file.

In a federated environment where all units (collectors and aggregators) are managed by one manager, all templates are shared by both collectors and aggregators and CAS data can be used in reporting or vulnerability assessments. When the collector and aggregator (or host where archived data is restored) are not part of the same management cluster the

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

templates are not shared and therefore CAS data cannot be used by vulnerability assessments even when the data is present, to remedy this use export/import of definitions to copy the templates from the collector to the aggregator (or restore target).

Monitored Entity

The actual entity being monitored, can be a File (its content and properties), Value of an Environment Variable or Windows Registry, Output of an OS command or Script or SQL statement.

CAS Instance

Application of a CAS Template Set on a specific Host (creating an Instance of that Template Set and applying it on a specific host).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Configuration Auditing System (3 of 3)

- **Configuration Auditing System:**
  - **CAS Hosts**
  - **CAS Reporting**
  - **CAS Status (see CAS Status Panel)**

Component	Description
	On the top row only of the panel, displays the CAS status on the Guardium appliance. Red: CAS is not running on this Guardium appliance. Green: CAS is active on this Guardium appliance.
	For each CAS host where this Guardium appliance is the active Guardium host, the status lights indicate whether CAS is connected: **Red**: Host and/or the CAS agent is offline or unreachable. **Green**: Host and CAS agent are online. **Yellow:** The Guardium appliance is a secondary for the CAS host.
(Reset)	Reset the CAS agent on this monitored system. This stops and restarts the CAS agent on the database server.
(Delete)	Remove this monitored system from CAS and also deleting the data on the appliance that was associated with the CAS client. This button is disabled if the CAS agent is running on this system. You must stop the CAS agent to use this button. See Stopping and Starting the CAS Agent, below.
	Each set of lights indicates the status of a CAS instance on the monitored system. If the owning monitored system status is red (indicating that the CAS agent is offline), ignore this set of status lights. **Red**: The instance is disabled. **Green**: The instance is enabled and online, and its configuration is synchronized with the Guardium appliance configuration. **Yellow**: The instance is enabled, but the instance configuration on the Guardium appliance does not match the instance configuration on the monitored system (it has been updated on the Guardium appliance, but that update has not been applied on the monitored system).
Refresh	Click the Refresh button to re-check the status of all servers in the list. This button does not stop and/or restart CAS on a database server – it only checks the connection between CAS on the Guardium appliance and CAS on each database server.

Note: The TAP_IP entry in the guard_tap.ini file is required. If TAP_IP is missing CAS will not start and an error message will be logged in the log file on the CAS client.

© Copyright IBM Corporation 2011, 2013

Figure 10-6. Configuration Auditing System (3 of 3) GU2022.0

Notes:

CAS Hosts

Once you have defined one or more CAS template sets, and have installed CAS on a database server, you are ready to configure CAS on that host. A CAS host configuration defines one or more CAS instances. Each CAS instance specifies a CAS template set, and defines any parameters needed to connect to the database. For each database server on which CAS is installed, there is a single CAS host configuration, which typically contains multiple CAS instances - for example, one CAS instance to monitor operating system items, and additional CAS instances to monitor individual database instances.

CAS Reporting

The admin user has access to all query builders and default reports. The admin role allows access to the default CAS reports, but not to the CAS query builders. The **cas** role allows access to both the default CAS reports and the query builders.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

CAS Status

By default, the functions described in this topic are available to the *admin* user, and users with the *admin* role. Open the Administrator portal and locate the Local Taps section of the Administration Console. If there is no Local Taps section, the unit type setting for this Guardium appliance needs to be changed. See the description of the store unit type command in the Configuration and Control CLI Commands topic for instructions on how to enable the Local Taps menu.

To monitor CAS status, select CAS Status in the Local Taps section of the Administration Console to open the Configuration Auditing System Status panel.

For each database server where CAS is installed and running, and where this Guardium appliance is configured as the active Guardium host, this panel displays the CAS status, and the status of each CAS instance configured for that database server.

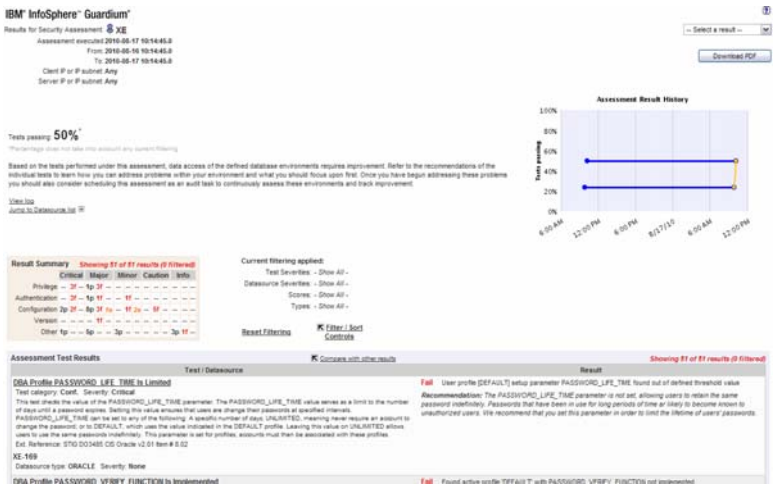
Regarding the sets of status lights on the Configuration Auditing System Status panel: when you hover the mouse over a set of status lights, a pop-up text box displays the current status. If you have trouble distinguishing the colors on your monitor, for all status light sets, the left-most light is always red, the right-most light is green, and on sets of three lights, the middle light is yellow.

The TAP_IP entry in the guard_tap.ini file is required. If TAP_IP is missing CAS will not start and an error message will be logged in the log file on the CAS client.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

VA

- Vulnerability Assessment
  - Runs a series of tests
  - Gives you a rating of the percentage of tests that were passed



© Copyright IBM Corporation 2011, 2013

Figure 10-7. VA GU2022.0

Notes:

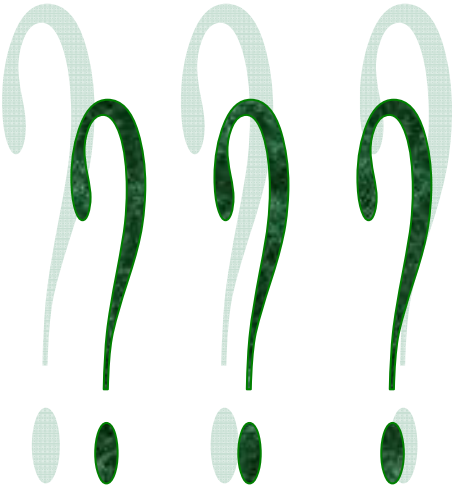
With Guardium's Vulnerability Assessment Tool, you choose from a series of tests. The results of the tests are displayed, along with a rating which represents a percentage of the tests that were "passed". A rating of 75% means that 25% of the tests *that were run* detected at least one area of vulnerability in your system.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Vulnerability Assessment (1 of 4)

- Three types of VA tests:
  - Query based
    - Missing patches, weak passwords, misconfigured privileges, etc
  - Behaviorial
    - Failed logins, after hour logins, administrative commands, etc
  - CAS based
    - Configuration and OS-level



© Copyright IBM Corporation 2011, 2013

Figure 10-8. Vulnerability Assessment (1 of 4) GU2022.0

Notes:

Guardium's Vulnerability Assessment tool uses three types of tests to evaluate the security of your database.

Query-based tests check for vulnerabilities such as missing patches, weak passwords, misconfigured privileges and default accounts

Behavioral tests are based on data gathered by Data Access Monitoring and look for items like excessive failed logins, clients executing administrative commands, and after-hours logins

CAS-based tests look for OS-level configuration vulnerabilities

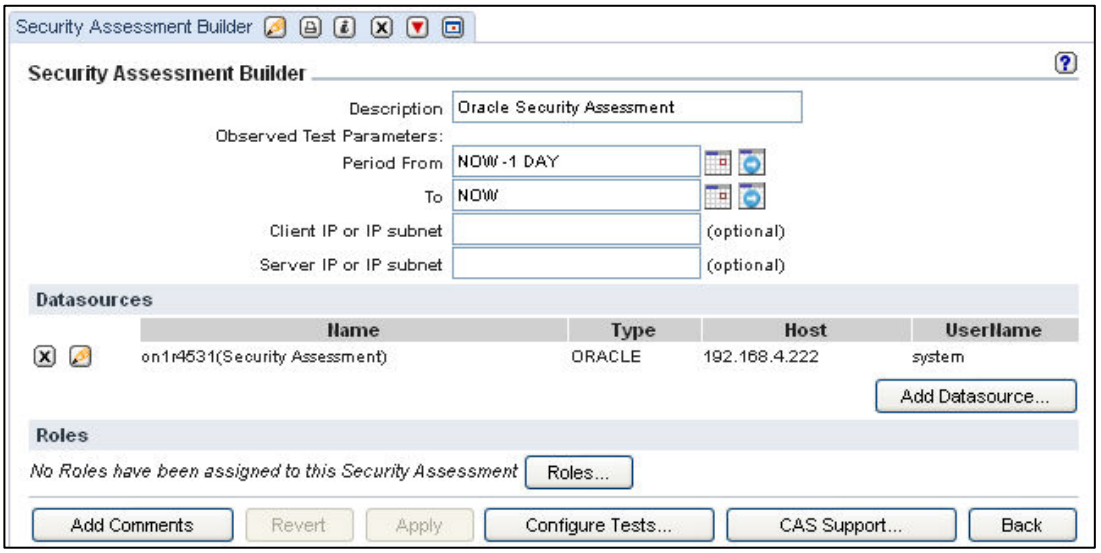
When the tests have completed, Guardium presents an overall report card along with details on each result including recommendations on resolving any issues.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Vulnerability Assessment (2 of 4)

Vulnerability Assessment

Security assessments allow organizations help identify and address database vulnerabilities in an automated fashion, which proactively improves configurations and hardens infrastructures.



© Copyright IBM Corporation 2011, 2013

Figure 10-9. Vulnerability Assessment (2 of 4) GU2022.0

Notes:

The Guardium Vulnerability Assessment solution is a licensed product that has an expiration date and is limited by a maximum number of datasources that can be defined and number of datasource scans (Metered scans). The **License valid until** date and **Metered scans left** can be seen on the **System Configuration** panel of the **Administrator Console.** A Vulnerability or Classification process with N datasources are counted as N scans every time they run.

Guardium Vulnerability Assessments requires access to the databases it evaluates. To do this, Guardium provides a set of SQL scripts (one script for each database type) that creates users and roles in the database to be used by Guardium.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Vulnerability Assessment (3 of 4)

- How does Guardium Vulnerability Assessments work?
- What are the Essential Security Testing methods?

- What are Predefined Assessment Tests?
- What are Behavioral Tests?

- What are Configuration Vulnerability Tests?
- What are Query-based Tests?

© Copyright IBM Corporation 2011, 2013

Figure 10-10. Vulnerability Assessment (3 of 4) GU2022.0

Notes:

How do Guardium Vulnerability Assessments Work

The Guardium Vulnerability Assessment application enables organizations to identify and address database vulnerabilities in a consistent and automated fashion. Guardium's assessment process evaluates the health of your database environment and recommends improvement by:

- Assessing system configuration against best practices and find vulnerabilities or potential threats to database resources, including configuration and behavioral risks.
  - For example, identifying all default accounts that haven't been disabled; checking public privileges and authentication methods chosen, etc.
- Finding any inherent vulnerabilities present in the IT environment, like missing security patches.
- Recommend and prioritizing an action plan based on discovered areas of most critical risks and vulnerabilities.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- Generating reports and recommendations provide guidelines on how to meet compliance changes and elevate security of the evaluated database environment.

What are the Essential Security Testing Methods

Guardium's Database Vulnerability Assessment combines three essential testing methods to guarantee full depth and breadth of coverage. It leverages multiple sources of information to compile a full picture of the security health of the database and data environment.

1. Agent-based-Using software installed on each endpoint (e.g. database server). They can determine aspects of the endpoint that cannot be determined remotely, such as administrator's access to sensitive data directly from the database console.
2. Passive detection-Discovering vulnerabilities by observing network traffic.
3. Scanning-Interrogating an endpoint over the network through credentialed access.

What are Predefined Assessment Tests

Predefined tests are designed to illustrate common vulnerability issues that may be encountered in database environments. Because of the highly variable nature of database applications and the differences in what is deemed acceptable in various companies or situations, some of these tests may be suitable for certain databases but totally inappropriate for others (even within the same company). Most of the predefined tests are customizable to meet requirement of your organization. Additionally, to keep your assessments current with industry best practices and protect against newly discovered vulnerabilities, Guardiums distribute new assessment tests and updates on quarterly bases as part of its Database Protection Subscription Service. Please refer to Guardium Administration Guide for more details.

What are Behavioral Tests

This set of tests assesses the security health of the database environment by observing database traffic in real-time and discovering vulnerabilities in the way information is being access and manipulated.

As an example, some of the behavioral vulnerability tests included are:

Default users access

Access rule violations

Execution of Admin, DDL, and DBCC commands directly from the database clients

Excessive login failures

Excessive SQL errors

After hours logins

Excessive administrator logins

Checks for calls to extended stored procedures

Checks that user ids are not accessed from multiple IP addresses

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

What are Configuration Vulnerability Tests

This set of assessments checks security-related configuration settings of target databases, looking for common mistakes or flaws in configuration create vulnerabilities.

As an example, the current categories, with some high-level tests, for configuration vulnerabilities include:

- Privilege - Object creation / usage rights; Privilege grants to DBA and individual users; System level rights
- Authentication - User account usage; Remote login usage; Password regulations
- Configuration - Database specific parameter settings; System level parameter settings
- Version - Database versions; Database patch levels
- Object - Installed sample databases; Recommended database layouts; Database ownership

What are Query Based Tests

Query-based tests are important as they allow a user to define tests that will be run against a database datasource and compare results against a predefined and expected value; allowing the user to check items such as database internals, structures, parameters, and even application data.

A query based tests are user defined tests that can be quickly and easy created by defining or modifying a SQL query, which will be run against database datasource and results compared to a predefined test value.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Vulnerability Assessment (4 of 4)

Integration with CAS

- Pre-configured and user-defined CAS templates play an important role in the identification of vulnerabilities and threats.
- With CAS, Guardium can identify vulnerabilities to the database in the OS level such as file permissions, ownership and environment variables.
- These tests can be seen through the CAS Template Set Definition panel and have the word 'Assessment' in their name.

© Copyright IBM Corporation 2011, 2013

Figure 10-11. Vulnerability Assessment (4 of 4) GU2022.0

Notes:

CAS-based Tests

A CAS-based test is either a pre-defined or user-defined test that is based on a CAS template item of type OS Script command and uses CAS collected data.

Users can specify which template item and test against the content of the CAS results.

Guardium also comes pre-configured with some CAS template items of type OS Script that can be used for creating a CAS-based test. These tests can be seen through the CAS Template Set Definition panel and have a name which contains the word 'Assessment'. For instance, the Unix/Oracle set for assessments is named 'Guardium Unix/Oracle Assessment'. Additionally, any template that is added that involves file permissions will also be used for permission and ownership checking.

Whether using a Guardium pre-configured or defining your own, once defined, these tests will appear for selection during the creation or modification of CAS-based tests.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Database Discovery and classification (1 of 2)

Database Auto-discovery

- Guardium's Auto-discovery application can be configured to probe the network, searching for and reporting on all databases discovered.
- Once an auto-discovery process has been defined, it can be run on demand or scheduled to be run on a periodic basis. There are two types of jobs that can be scheduled for each process:
  - A **scan** job scans each specified host (or hosts in a specified subnet), and compiles a list of open ports from the list of ports specified for that host. A scan job must be run before running the second type of job.
  - A **probe** job uses the list of open ports compiled during the latest completed scan only. The probe job determines if there are database services running on those ports. You can view the results of this job on the Databases Discovered predefined report.

© Copyright IBM Corporation 2011, 2013

Figure 10-12. Database Discovery and classification (1 of 2) GU2022.0

Notes:

Database Auto-discovery

Sometimes a new database is introduced into a production environment outside of the normal control mechanisms. For example, the new database might be part of an application package from a software vendor. In older installations some databases may have been left unmonitored and "forgotten," because the data and/or activities performed on it were not seen as a risk when the database was implemented.

Or in another case a rogue DBA might create a new instance of the database and do with it as he or she pleases, without being monitored.

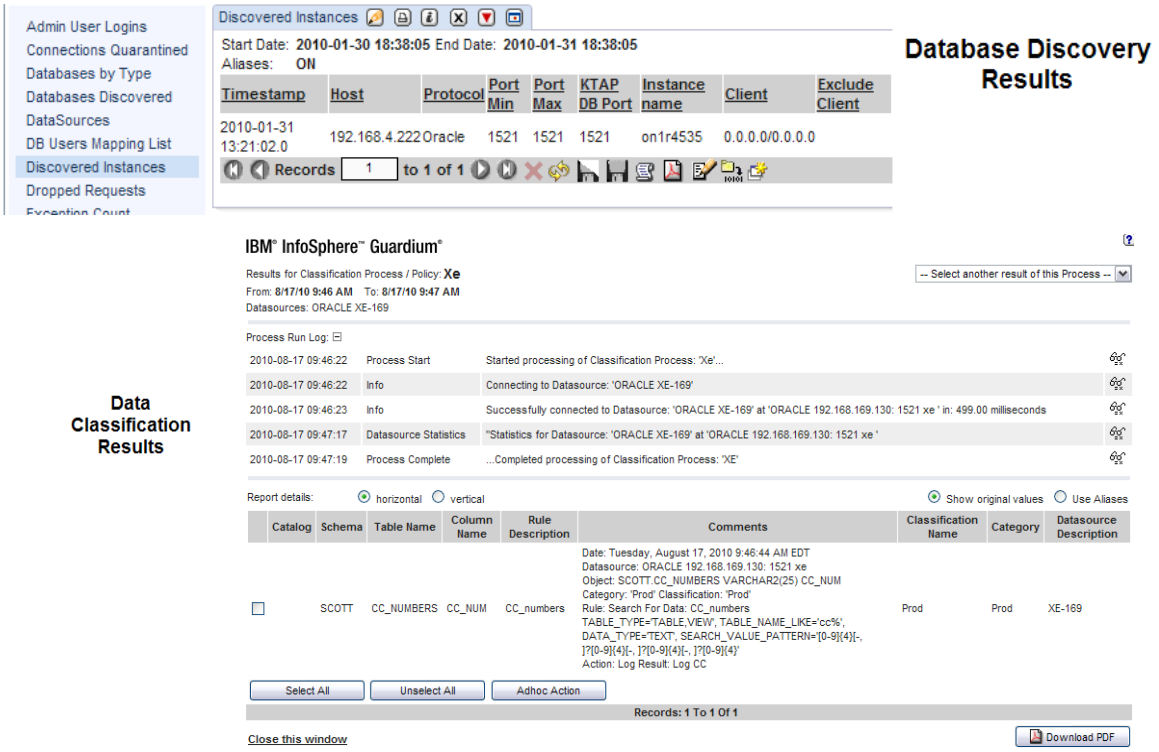
The two jobs can be scheduled individually, or the auto-discovery process can be defined to run the probe job as soon as the scan job completes.

Because the processes of scanning and probing ports can take time, the progress of an auto-discovery process can be displayed at any time (by clicking the Progress/Summary button).

Once the jobs have been completed, the results can be viewed using predefined reports.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Database Discovery and classification (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 10-13. Database Discovery and classification (2 of 2) GU2022.0

Notes:

Due to the complexity of some environments and other factors, such as mergers and acquisitions, some companies do not have a full inventory of their database servers and do not understand where all of their sensitive data resides. Database Discovery probes a network to identify servers running database services. Data Classification scans databases to find and classify any objects or fields containing sensitive data.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. A CAS template set is taylored to:
   a. An Operating System (such as Unix)
   b. An Operating System and Database (such as Unix and DB2)
   c. Both a and b
   d. Neither a nor b
2. True or false: You can modify one or more of the CAS default templates.
3. CAS has been configured with a period of 2 hours. The last set of tests ran at 10:30 am. When will the next set of tests run?
   a. At 11:30 am
   b. At 12:30 pm
   c. Between 11:30 am and 12:30 pm
   d. Between 10:30 am and 12:30 pm

© Copyright IBM Corporation 2011, 2013

Figure 10-14. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. A CAS template set is tailored to:
   a. An Operating System (such as Unix)
   b. An Operating System and Database (such as Unix and DB2)
   c. **Both a and b**
   d. Neither a nor b
2. True **or false**: You can modify one or more of the CAS default templates.
3. CAS has been configured with a period of 2 hours. The last set of tests ran at 10:30 am. When will the next set of tests run?
   a. At 11:30 am
   b. At 12:30 pm
   c. Between 11:30 am and 12:30 pm
   d. **Between 10:30 am and 12:30 pm**

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Checkpoint (2 of 2)

4. What are the three categories of VA tests?

5. How often are the Guardium assessment tests updated by IBM?
   a. Annually
   b. Quarterly
   c. Monthly
   d. Weekly

6. True or false: You need only CAS or only VA, not both.

© Copyright IBM Corporation 2011, 2013

Figure 10-15. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

4. What are the three categories of VA tests?

   Query based, Behavioral, CAS based

5. How often are the Guardium assessment tests updated by IBM?

   a. Annually

   b. **Quarterly**

   c. Monthly

   d. Weekly

6. True or **false**: You need only CAS or only VA, not both.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand the major components of the Configuration Auditing System (CAS)
- Understand the value of Vulnerability Assessment
- Understand why Database Discovery is needed

© Copyright IBM Corporation 2011, 2013

Figure 10-16. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercises 8 and 9** in the Exercise Guide.

© Copyright IBM Corporation 2011, 2013

Figure 10-17. Exercise GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (1 of 2)

1. A CAS template set is taylored to:
   a. An Operating System (such as Unix)
   b. An Operating System and Database (such as Unix and DB2)
   c. Both a and b
   d. Neither a nor b
2. True **or false**: You can modify one or more of the CAS default templates.
3. CAS has been configured with a period of 2 hours. The last set of tests ran at 10:30 am. When will the next set of tests run?
   a. At 11:30 am
   b. At 12:30 pm
   c. Between 11:30 am and 12:30 pm
   d. Between 10:30 am and 12:30 pm

© Copyright IBM Corporation 2011, 2013

Figure 10-18. Checkpoint solutions (1 of 2) GU2022.0

Notes:

Write your answers here:

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (2 of 2)

4. What are the three categories of VA tests?

   Query based, Behavioral, CAS based

5. How often are the Guardium assessment tests updated by IBM?

   a. Annually

   b. Quarterly

   c. Monthly

   d. Weekly

6. True or **false**: You need only CAS or only VA, not both.

© Copyright IBM Corporation 2011, 2013

Figure 10-19. Checkpoint solutions (2 of 2) GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 11. Custom Query and Report Building

Estimated time

01:45

What this unit is about

This unit describes how to create custom queries and reports.

What you should be able to do

After completing this unit, you should be able to:

- Understand domains, entities, and attributes
- Create custom queries and reports

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand domains, entities, and attributes
- Create custom queries and reports

© Copyright IBM Corporation 2011, 2013

Figure 11-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

11.1. Query overview and creating a simple query

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Query overview and creating a simple query

After completing this topic, you should be able to:

- Create a simple query
- Add fields and conditions to a query
- Understand the domains, entities and attributes
- Add a query to a pane
- View a report and change a report's run-time parameters

© Copyright IBM Corporation 2011, 2013

Figure 11-2. Query overview and creating a simple query GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Creating a custom query

- Choose the domain
- Name the query
- Select the main entity
- Identify fields to be listed
- Add a query condition
- Generate the report
- View the results

© Copyright IBM Corporation 2011, 2013

Figure 11-3. Creating a custom query GU2022.0

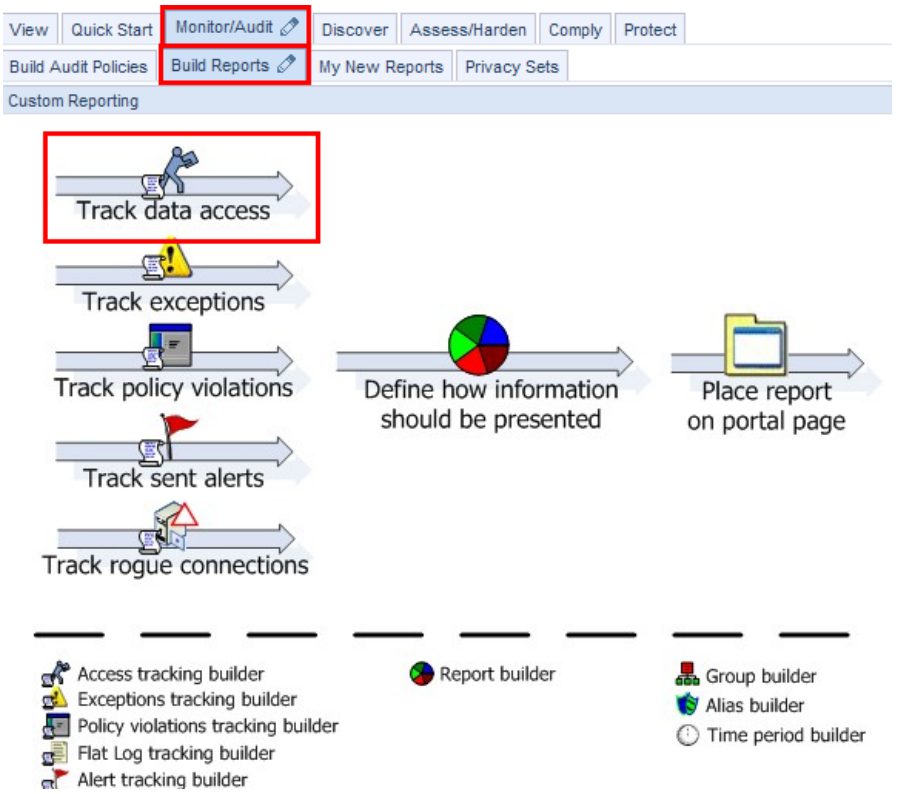
Notes:

This topic will cover the seven steps required to create a new query:

- Choose the domain
- Name the query
- Select the main entity
- Identify fields to be listed
- Add a query condition
- Generate the report
- View the results

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Track data access



© Copyright IBM Corporation 2011, 2013

Figure 11-4. Track data access GU2022.0

Notes:

To build a new custom query, go to **Monitor/Audit** > **Build Reports**. On the left hand column there are a number of buttons that begin with 'Track' or contain the phase 'tracking builder'. These buttons open the query builder for a specific domain. For example, **Track data access** will open the query builder for the **Access Domain**.

Domains will be discussed on the next page.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Domain

A domain is a view of the data

There are 3 domains:

- Standard Domains, for example:
  - Access (all monitored SQL requests)
  - Exceptions (from database servers or appliance components)
  - Alerts, Policy Violations, and so on
- Administrator Domains, for example:
  - Aggregation/Archive (archive, backup, restore, and so on)
  - Logins, Activity, and so on
- Optional Product Domains, for example:
  - Classifier Results
  - CAS Changes (database server configuration file changes, for example)

© Copyright IBM Corporation 2011, 2013

Figure 11-5. Domain GU2022.0

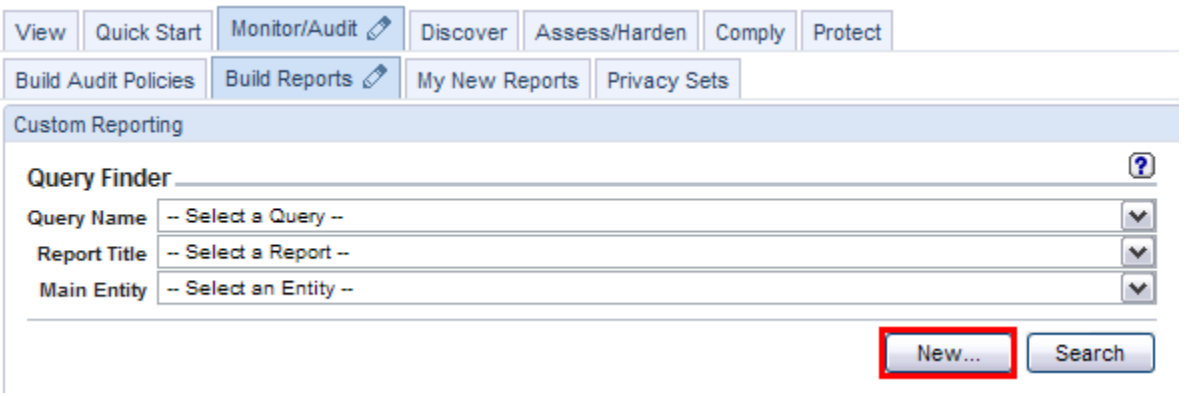
Notes:

A domain provides a view of the stored data and has the following characteristics:

- Each domain contains a set of data related to a specific purpose or function (data access, exceptions, policy violations, and so forth)
- Each domain contains one or more entities. An entity is a set of related attributes (basically a field value).
- A query returns data from one domain only. When the query is defined, one entity within that domain is designated as the main entity of the query. Each row of data returned by a query will contain a count of occurrences of the main entity matching the values returned for the selected attributes, for the requested time period. This allows for the creation of two-dimensional reports from entities that do not have a one-to-one relationship.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Query finder: New query



© Copyright IBM Corporation 2011, 2013

Figure 11-6. Query finder: New query GU2022.0

Notes:

After selecting a domain (in this example we chose the *Access* domain by choosing “Track Access Data” on the Build Reports pane), you will be brought to the *Query Finder* for that domain. To create a new query press the **New…** button.

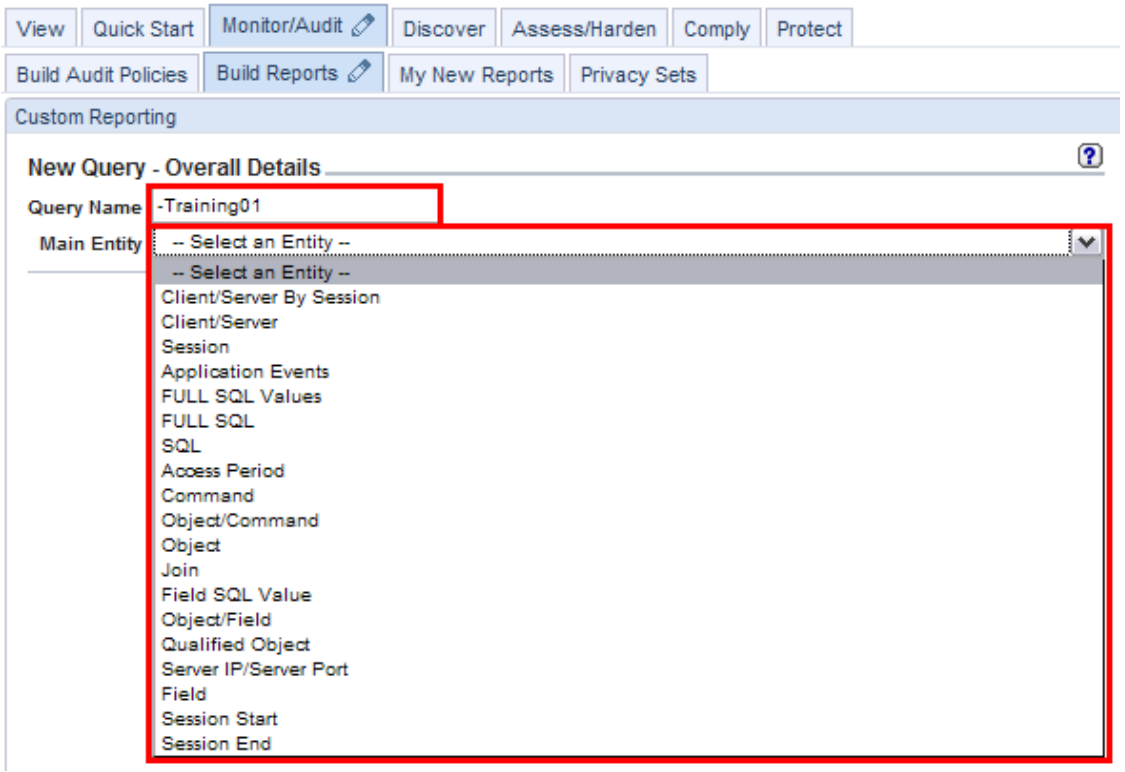
Alternatively, choose to **Search** for an existing query. Existing custom queries can be modified directly or cloned and saved as a new query. Existing built-in queries cannot be modified directly. If you would like to change a built-in query, you must clone it.

In our example, we will be create a **New…** query.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

New query: Name and main entity



© Copyright IBM Corporation 2011, 2013

Figure 11-7. New query: Name and main entity GU2022.0

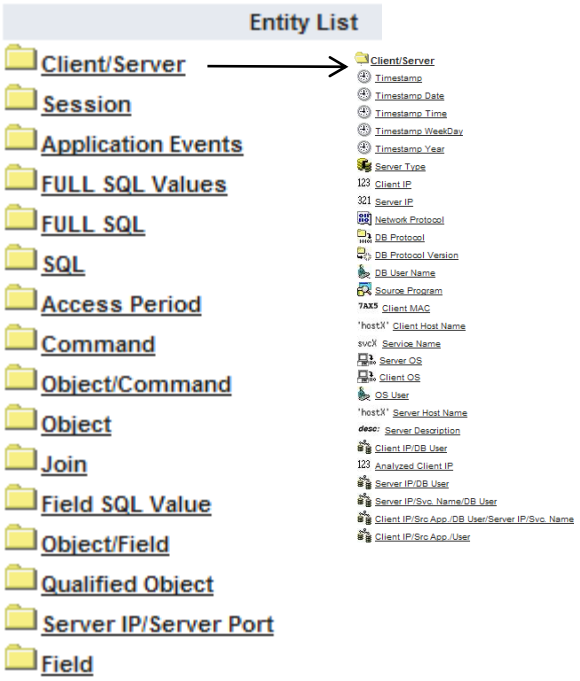
Notes:

To create a new query, you must:

- Enter a **Query Name**. Note, you should use a naming a convention to differentiate your custom queries from the built-in queries. In this example, we will simply add a dash (-). This will also cause the query to appear at the top of the list.
- Choose a **Main Entity**, which will be explained in the next few pages.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Main entity: About entities



© Copyright IBM Corporation 2011, 2013

Figure 11-8. Main entity: About entities GU2022.0

Notes:

Each domain contains one or more entities. An **entity** is a set of related attributes. An **attribute** is basically a field value.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Access domain entities

- Client/Server
- Session
- Application Events
- Full SQL Values
- Full SQL
- SQL
- Access Period
- Command
- Object
- Object-Command
- Field
- Field SQL Value
- Object-Field

© Copyright IBM Corporation 2011, 2013

Figure 11-9. Access domain entities GU2022.0

Notes:

Below are the entities within the Access domain. The access domain is where all SQL requests are logged.

- **Client/Server**: Client and database server connection info (IPs, OS, etc.)
- **Session**: Database name, session start and end times
- **Application Events**: Events from the Guardium API
- **Full SQL Values**: Values logged separately for faster search
- **Full SQL**: The full SQL string (with values)
- **SQL**: The SQL request (no values)
- **Access Period**: When – Logging granularity
- **Command**: SQL command
- **Object**: SQL object
- **Object-Command**: Command detected in object

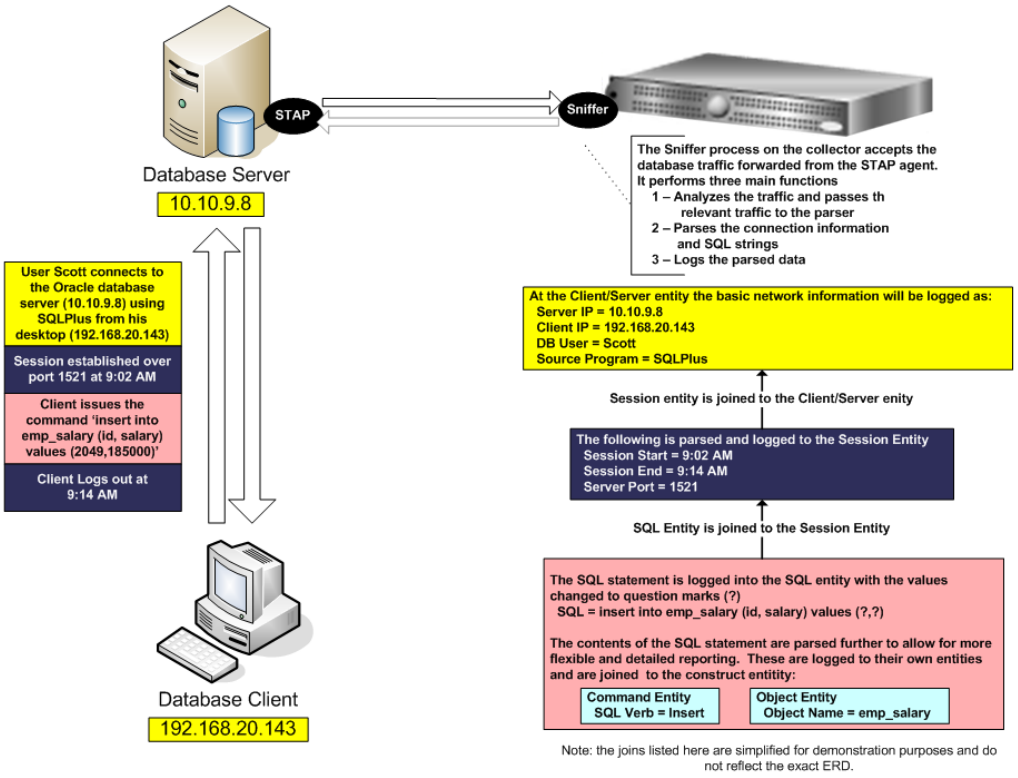
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Field**: Field
- **Field SQL Value**: Field value logged separately for faster search
- **Object-Field**: Field detected in object

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Logging and parsing


STAP
Sniffer
Database Server
10.10.9.8
The Sniffer process on the collector accepts the database traffic forwarded from the STAP agent. It performs three main functions
1 – Analyzes the traffic and passes th relevant traffic to the parser
2 – Parses the connection information and SQL strings
3 – Logs the parsed data
User Scott connects to the Oracle database server (10.10.9.8) using SQLPlus from his desktop (192.168.20.143)
Session established over port 1521 at 9:02 AM
Client issues the command 'insert into emp_salary (id, salary) values (2049,185000)'
Client Logs out at 9:14 AM
At the Client/Server entity the basic network information will be logged as:
Server IP = 10.10.9.8
Client IP = 192.168.20.143
DB User = Scott
Source Program = SQLPlus
Session entity is joined to the Client/Server enity
The following is parsed and logged to the Session Entity
Session Start = 9:02 AM
Session End = 9:14 AM
Server Port = 1521
SQL Entity is joined to the Session Entity
The SQL statement is logged into the SQL entity with the values changed to question marks (?)
SQL = insert into emp_salary (id, salary) values (?,?)
The contents of the SQL statement are parsed further to allow for more flexible and detailed reporting. These are logged to their own entities and are joined to the construct entitity:
Command Entity
SQL Verb = Insert
Object Entity
Object Name = emp_salary
Database Client
192.168.20.143
Note: the joins listed here are simplified for demonstration purposes and do not reflect the exact ERD.

© Copyright IBM Corporation 2011, 2013

Figure 11-10. Logging and parsing GU2022.0

Notes:

We viewed this slide in the policy unit and is repeated here to help visualize the entity structure.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Entity Hierarchy

	Entities	Description
1	Client/Server Session	Each client/server connection has one or more sessions. Each session has one of more requests.
2	Application Events	Each request has some combination of this entity.
3	Full SQL Values Full SQL SQL Access Period	Each request has some combination of these entities.
4	Command	Each request may contain commands.
5	Object	Each command may contain objects.
6	Object-Command Field Field SQL Value Object-Field	Each object may contain these entities.

© Copyright IBM Corporation 2011, 2013

Figure 11-11. Entity Hierarchy GU2022.0

Notes:

The data within the Guardium database is logged in a hierarchal manner. Entities higher in the entity structure may contain multiple instances of entities lower in the hierarchy. For example:

- One Client/Server connection can contain multiple sessions.
- One SQL request (complete SQL statement) can contain many commands
- One command may reference multiple objects
- A single object contains multiple fields

This is important because when creating a query, you must choose one entity as the ‘main’ entity and what you choose as the main entity will affect how the data is presented.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Main entity: Effects

The **main entity** that you select for a query determines:

- The **level of detail** for the report
- The **total count**
- The **time fields** against which the **Period From** and **Period To** run-time parameters will be compared

© Copyright IBM Corporation 2011, 2013

Figure 11-12. Main entity: Effects GU2022.0

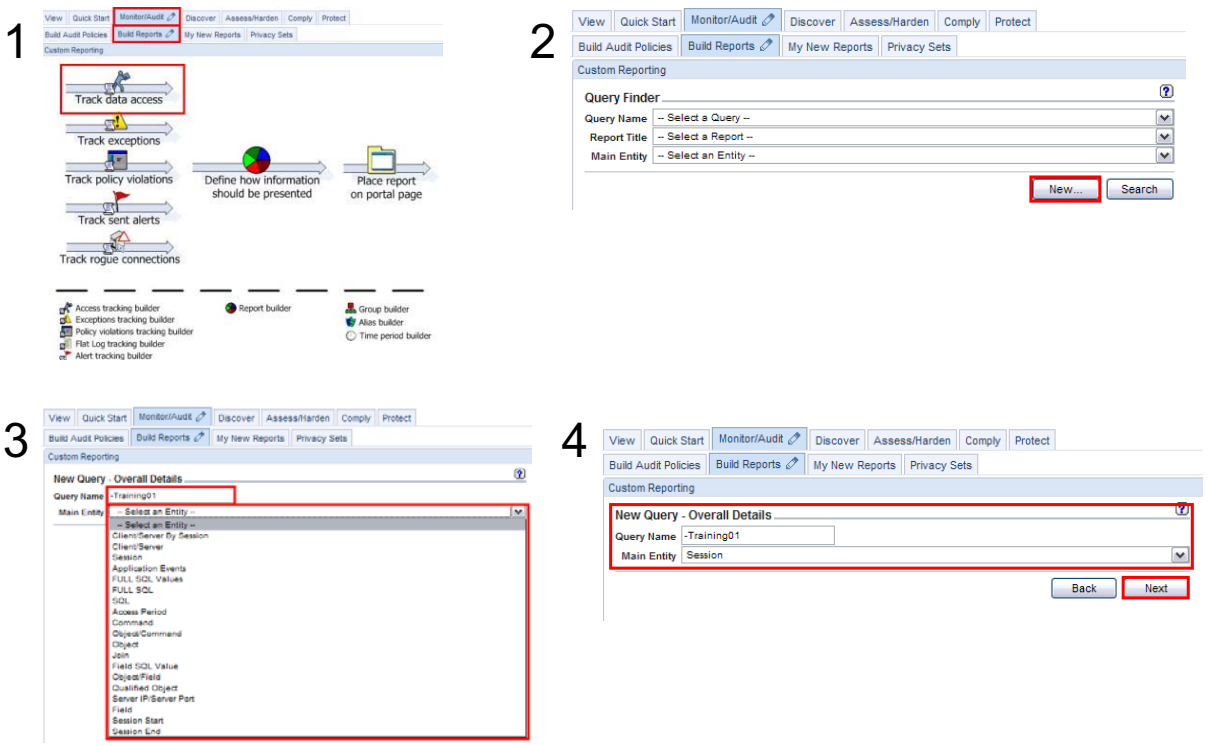
Notes:

The main entity determines:

- The **level of detail** for the report. There will be one row of data for each occurrence of the main entity included in the report. The location of the main entity within the hierarchy of entities is important in terms of what values can be displayed. The attributes for any entities below the main entity can be counted, but not displayed (since there may be many occurrences for each row).
- The **total count,** added as the last column of the report, which is a count of instances of the main entity included on that row of the report.
- The **time fields** against which the **Period From** and **Period To** run-time parameters will be compared to select the rows of the report. When defining a Query (in the Query Builder) the system uses the main entity (among other parameters) to determine which time fields will be used when defining the Period From and Period To of the report/alert using this query. When applicable the Period Start/Period End from the 'Access Period' entity is usually used, in other cases it will chose period values according to the main entity.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

New query steps summary



© Copyright IBM Corporation 2011, 2013

Figure 11-13. New query steps summary GU2022.0

Notes:

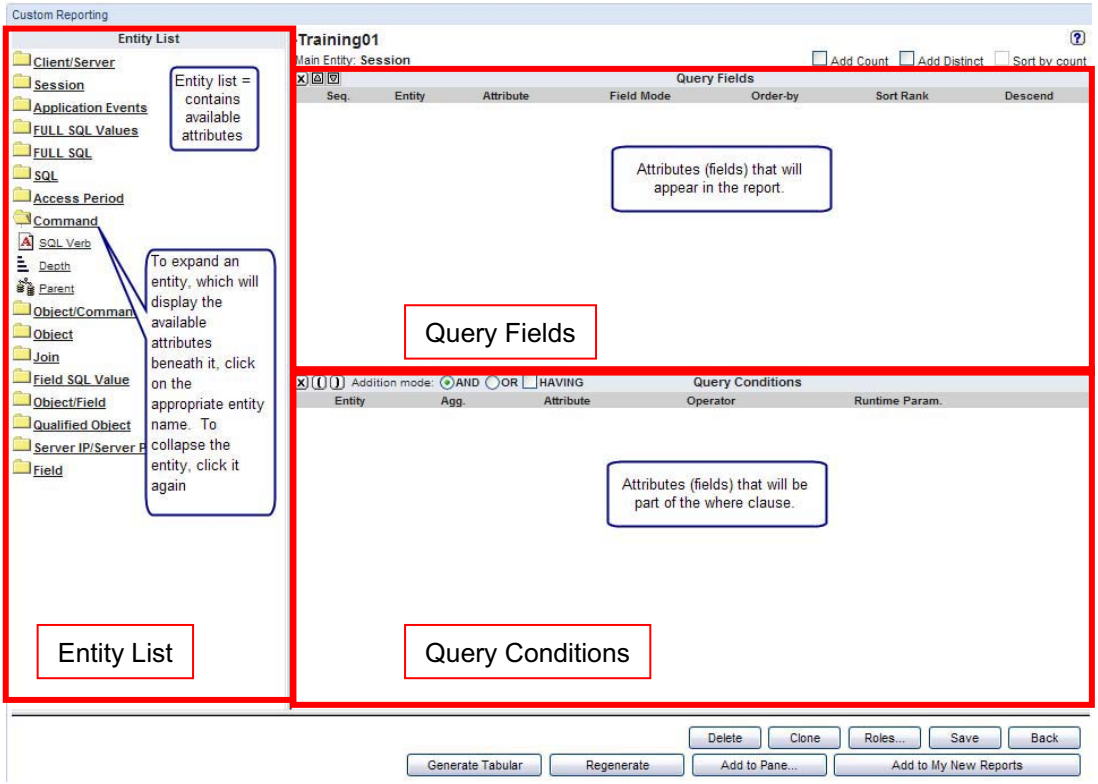
This is a summary of the steps we have taken so far to create a new query:

1. Go to **Monitor/Audit** > **Build Reports** and press the **Track data access** button
2. Click **New…**
3. Enter a **Query Name** and choose a **Main Entity**
4. Press **Next**

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Custom query builder



© Copyright IBM Corporation 2011, 2013

Figure 11-14. Custom query builder GU2022.0

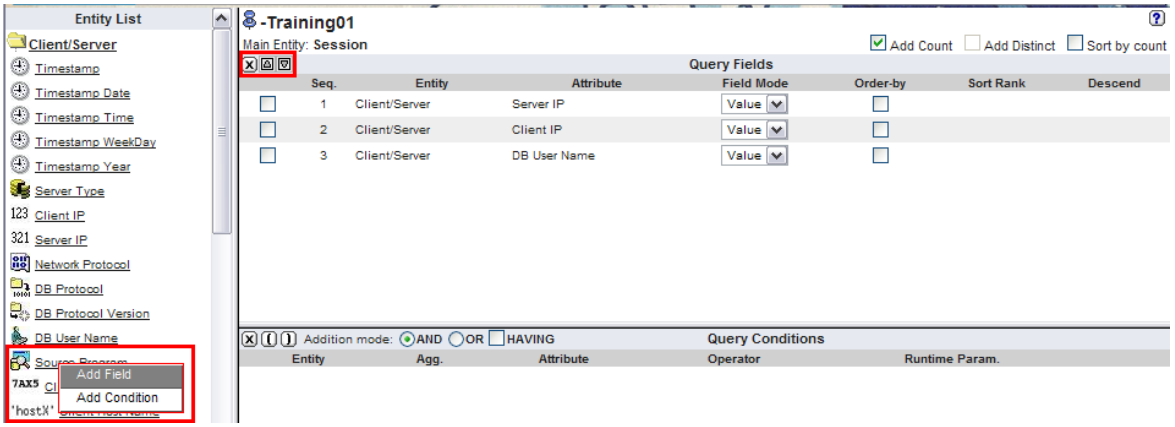
Notes:

The custom query builder is composed of three panes

- **Entity List** allows you to select attributes to add the to query, either as fields in the report or query conditions
- **Query Fields** are the fields that will appear in the report
- **Query Conditions** contains the where clause of the query

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Adding fields



© Copyright IBM Corporation 2011, 2013

Figure 11-15. Adding fields GU2022.0

Notes:

Add Fields to the Query Fields Pane

There are two ways to add a field to the Query Fields pane:

- Pop-Up Menu Method:
  - Click on the field to be added.
  - Select **Add Field** from the popup menu.
- Drag-and-Drop Method:
  - Click on the icon to the left of the field (not on the field name).
  - Drag the icon to the Query Fields list and release it.

Regardless of the method used, the field will be added to the end of the list.

Move or Remove Fields in the Query Fields Pane

To move a field in the Query Fields pane:

- Mark the checkbox in the left-most column for the field.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

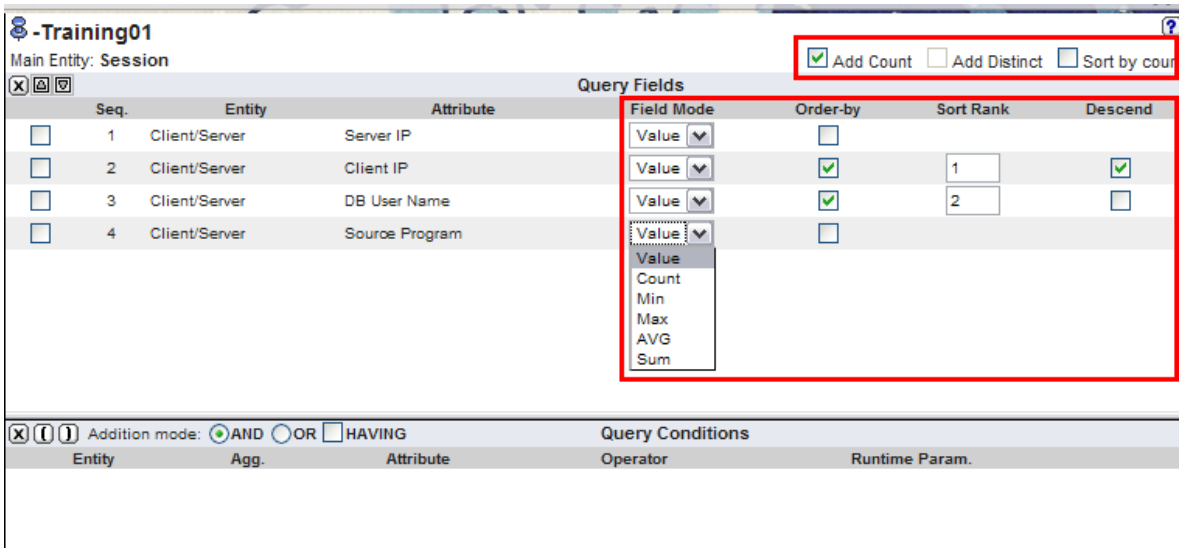
- Use the arrow buttons to move the field to the desired location.

To remove a field from the Query Fields pane:

- Mark the checkbox in the left-most column for the field.
- Click the '**x**' button to remove the field.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Changing query settings



© Copyright IBM Corporation 2011, 2013

Figure 11-16. Changing query settings GU2022.0

Notes:

Other Query Field options include

- **Field Mode** - indicates what to print for the field: its Value, or the Count (count is a count of distinct values), Min, Max, Average (AVG) or Sum for the row. The Value option is not available for attributes from entities lower than the main entity in the entity hierarchy for the domain.
- **Order-by** – check the corresponding box to sort by a specific field. By default, query data is sorted in ascending order by attribute value, with the sort keys ordered as the attributes appear in the query. If aliases are being used, they are ignored for sorting purposes; the actual data values are always used for sorting. Attributes for which values are computed by the query (Count, Min, Max, or Avg) cannot be sorted.
- **Sort Rank** – when the order-by box is checked enter to number here to indicate the rank by which the field will be sorted, relative to the other sorted fields
- **Descend** – (optional) controls whether the field will sort in ascending or descending order

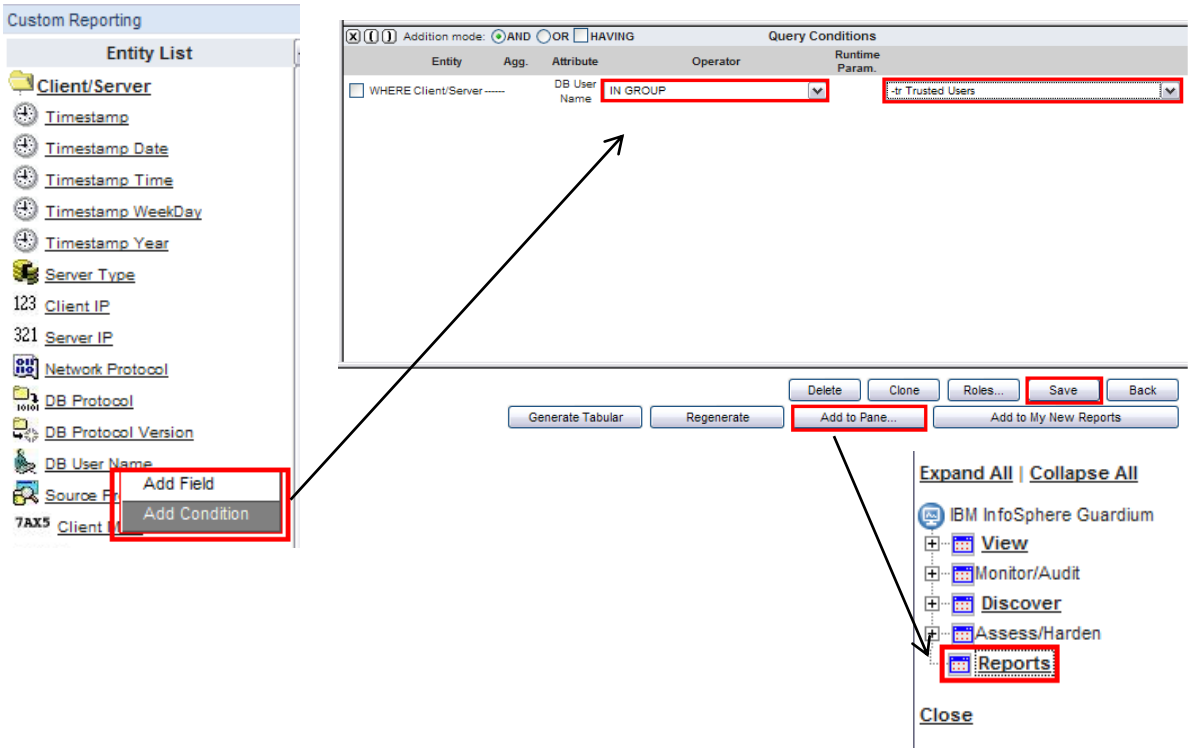
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Add Count** – adds a count of distinct instances, as the last column of the report
- **Add Distinct** - adds or drops the ability to display one-row-per-value in the report
- **Sort by count** – will cause the report to sort by the count field

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Adding a condition, saving and publishing report



© Copyright IBM Corporation 2011, 2013

Figure 11-17. Adding a condition, saving and publishing report GU2022.0

Notes:

This unit will cover query conditions in great detail but in this example we will show how to add a simple condition and save the report.

Adding a condition:

- To add a condition, click on the attribute in which you are interested and choose **Add Condition** (alternatively drag and drop the attribute). In this example we will choose **DB User Name**.
- Choose and operator; choose **IN GROUP** and choose **–tr Trusted Users**

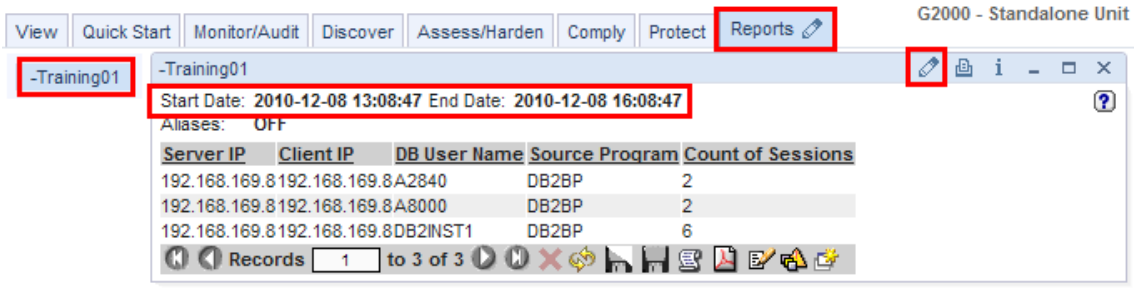
To save the report

- Press the **Save** button
- Press the **Add to Pane…** button and in the pop-up window select the **Pane** on which you would like to add the report. You may add the report to any pane defined as a *menu pane*.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Viewing a report



© Copyright IBM Corporation 2011, 2013

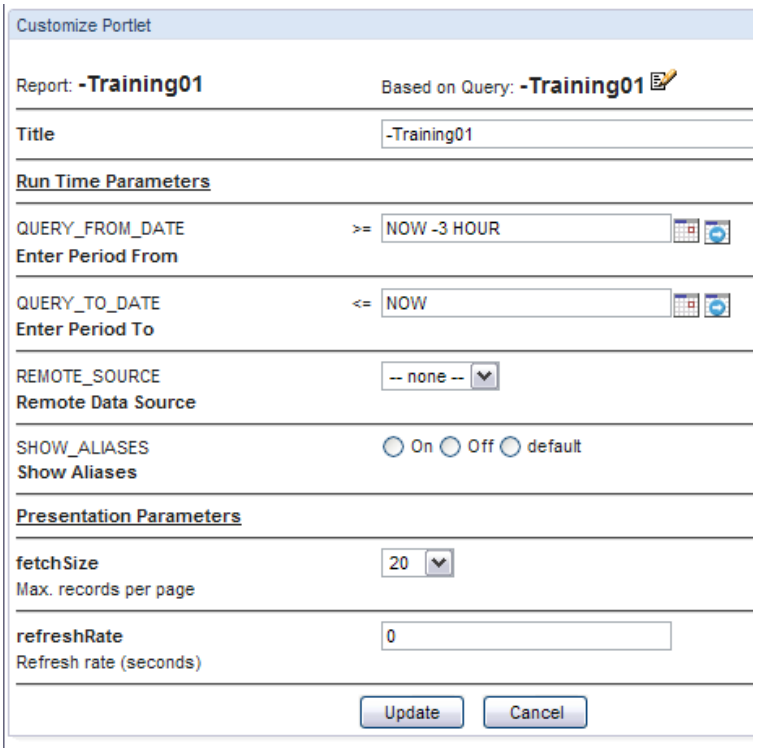
Figure 11-18. Viewing a report GU2022.0

Notes:

After adding the report to a pane, go to that pane to view the results. By default the report will show the results for the previous three hours. To modify the time frame, click the **Customize** icon.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Customize screen



© Copyright IBM Corporation 2011, 2013

Figure 11-19. Customize screen GU2022.0

Notes:

The **Customize Portlet** screen allows you to change both the data returned by the report and how it is presented. There are two types of report parameters:

- A **run-time parameter** provides a value to be used in a query condition. There is a default set of run-time parameters for all queries and any number of custom run-time parameters can be defined in the query used by the report. Custom run-time parameters will be covered later in this unit.
- A **presentation parameter** describes a physical characteristic the report; for example whether a graphical report includes a legend or labels, or what colors to use for an element. All presentation parameters are provided with initial settings when you define a report.

Standard run-time parameters:

- **QUERY_FROM_DATE** - The starting date and time for the report.
- **QUERY_TO_DATE** - This is the ending date for the report.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

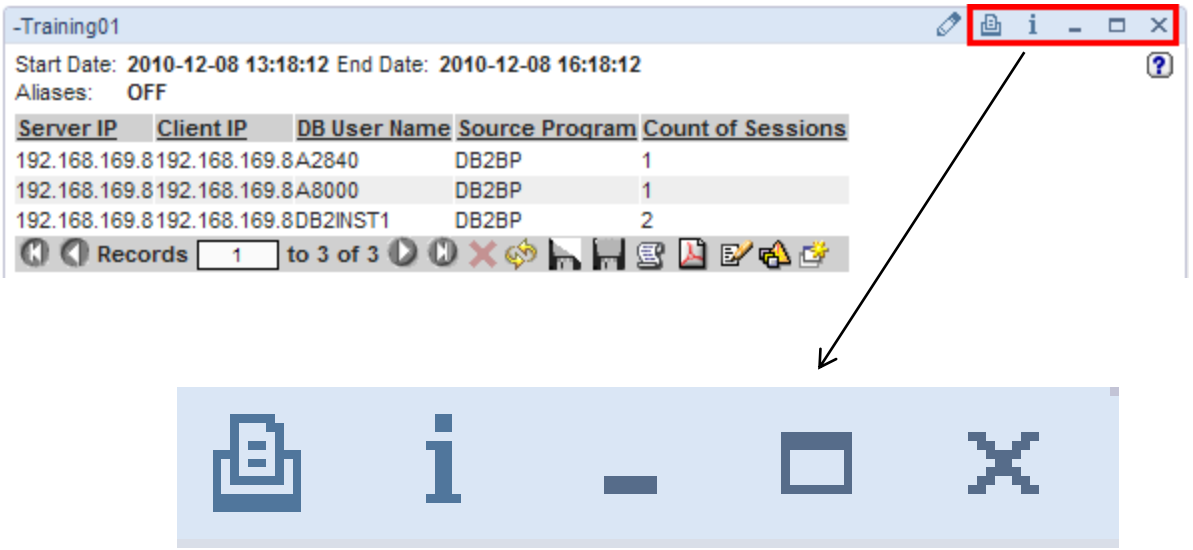
- **REMOTE_SOURCE** - In a Central Manager environment, you can run a report on a managed unit by selecting that Guardium appliance from the Remote Data Source list.

Standard presentation parameters:

- **fetchSize** - The number of rows to display in the report portal panel.
- **refreshRate** - The number of seconds after which the data is to be refreshed. Zero means that the data will not be refreshed.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Pane buttons



© Copyright IBM Corporation 2011, 2013

Figure 11-20. Pane buttons GU2022.0

Notes:

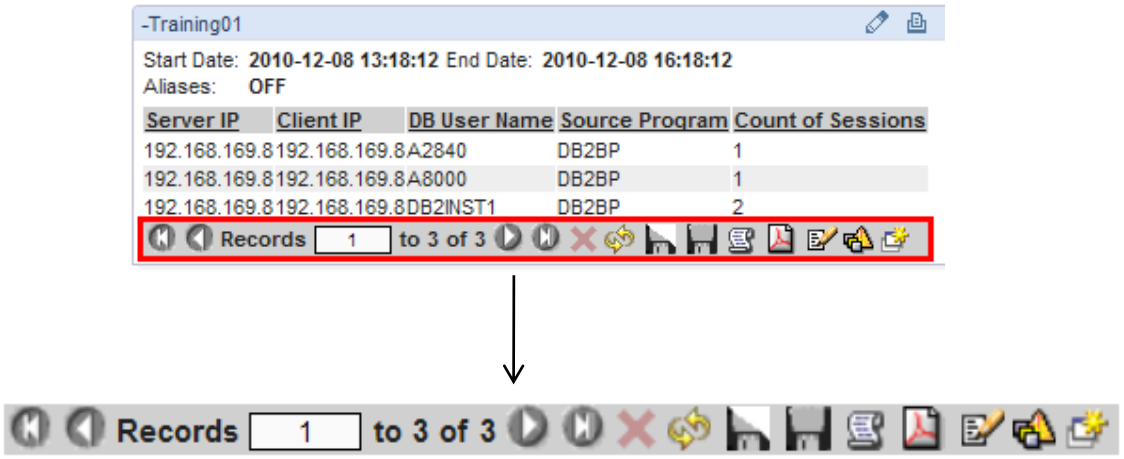
Other portlet buttons include (from left to right above):

- **Print-Friendly Format** – Displays the panel contents in a printer-friendly format (which minimizes the use of curved lines).
- **Information** – Displays information about the portlet.
- **Minimize -** Minimize the portlet. When minimized, the Minimize and Maximize buttons are replaced by a **Restore** button
- **Maximize** – Maximizes the report window.
- **Close** – Removes the portlet from the current pane.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Report buttons



© Copyright IBM Corporation 2011, 2013

Figure 11-21. Report buttons GU2022.0

Notes:

Other report buttons, available at the bottom of all reports include (from left to right):

- **Navigation buttons** – arrows allowing you to move from page to page within the displayed report. You can also enter a number in the box next to 'Records' to go directly to a specific page.
- **Stop –** The red 'x' button will stop the report generations
- **Refresh**– The yellow arrows refreshes the current report
- The first disk icon (with the white corner) will **download the data currently displayed** on the portal in CSV format
- The second disk icon **downloads the entire report** in CSV format
- The printer icon will open a **printer-friendly** window
- The **pdf** icon will save the report as a **PDF** file
- The paper and pencil icon will **open the query builder** for this report's underlying query

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- The second button from the end will create an **ad hoc audit process**, allowing long-running queries to be processed in the background as an audit process
- The last button will open the report in a **new window**

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Checkpoint

1. True or false: A query can access the data in only one domain.
2. Why should you use a dash (-) or other special character as part of your query's name?
3. Which of the following represents the correct heirarchy?
   a) Attribute -> Entity -> Domain
   b) Entity -> Domain -> Attribute
   c) Domain -> Attribute -> Entity
   d) Domain -> Entity -> Attribute
4. You have set SQL as your Access Domain. Can you still ask for a count of something in the Session entity?
5. In terms of an SQL select statement, Query Fields go on the _____ clause and Query Conditions go on the _____ clause.
6. True or false: On the customization screen, you can change the date range for the main entity.

© Copyright IBM Corporation 2011, 2013

Figure 11-22. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. **True** or false: A query can access the data in only one domain.
2. Why should you use a dash (-) or other special character as part of your query's name?

   To differentiate them from built-in queries and to move them to the top of the sorted list.
3. Which of the following represents the correct heirarchy?
   a. Attribute -> Entity -> Domain
   b. Entity -> Domain -> Attribute
   c. Domain -> Attribute -> Entity
   d. **Domain -> Entity -> Attribute**
4. You have set SQL as your Access Domain. Can you still ask for a count of something in the Session entity?

   Yes, since Session is above SQL.
5. In terms of an SQL select statement, Query Fields go on the **SELECT** clause and Query Conditions go on the **WHERE** clause.
6. **True** or false: On the customization screen, you can change the date range for the main entity.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Create a simple query
- Add fields and conditions to a query
- Understand the domains, entities and attributes
- Add a query to a pane
- View a report and change the reports run-time parameters

© Copyright IBM Corporation 2010, 2013

Figure 11-23. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. **True** or false: A query can access the data in only one domain.
2. Why should you use a dash (-) or other special character as part of your query's name? **To differentiate them from built-in queries and to move them to the top of the sorted list.**
3. Which of the following represents the correct heirarchy?
   a) Attribute -> Entity -> Domain
   b) Entity -> Domain -> Attribute
   c) Domain -> Attribute -> Entity
   d) Domain -> Entity -> Attribute
4. You have set SQL as your Access Domain. Can you still ask for a count of something in the Session entity? **Yes, since Session is above SQL.**
5. In terms of an SQL select statement, Query Fields go on the **SELECT** clause and Query Conditions go on the **WHERE** clause.
6. **True** or false: On the customization screen, you can change the date range for the main entity.

© Copyright IBM Corporation 2011, 2013

Figure 11-24. Checkpoint solutions GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 10** in the Exercise Guide. Alternately, you can wait and do Exercises 10, 11, and 12 at the end of this unit.

© Copyright IBM Corporation 2011, 2013

Figure 11-25. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

11.2. Query conditions

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Query conditions

After completing this topic, you should be able to:

- Add conditions to queries
- Use AND and OR clauses
- Use parentheses in queries
- Add a query to a pane
- Create custom run-time parameters

© Copyright IBM Corporation 2010, 2013

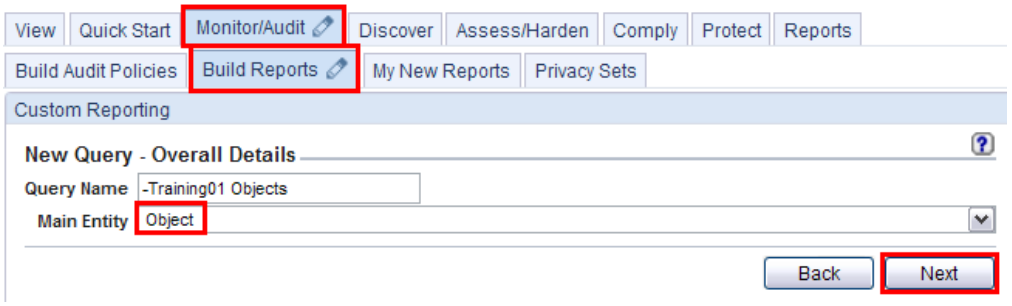
Figure 11-26. Query conditions GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

New query: Object main entity



© Copyright IBM Corporation 2011, 2013

Figure 11-27. New query: Object main entity GU2022.0

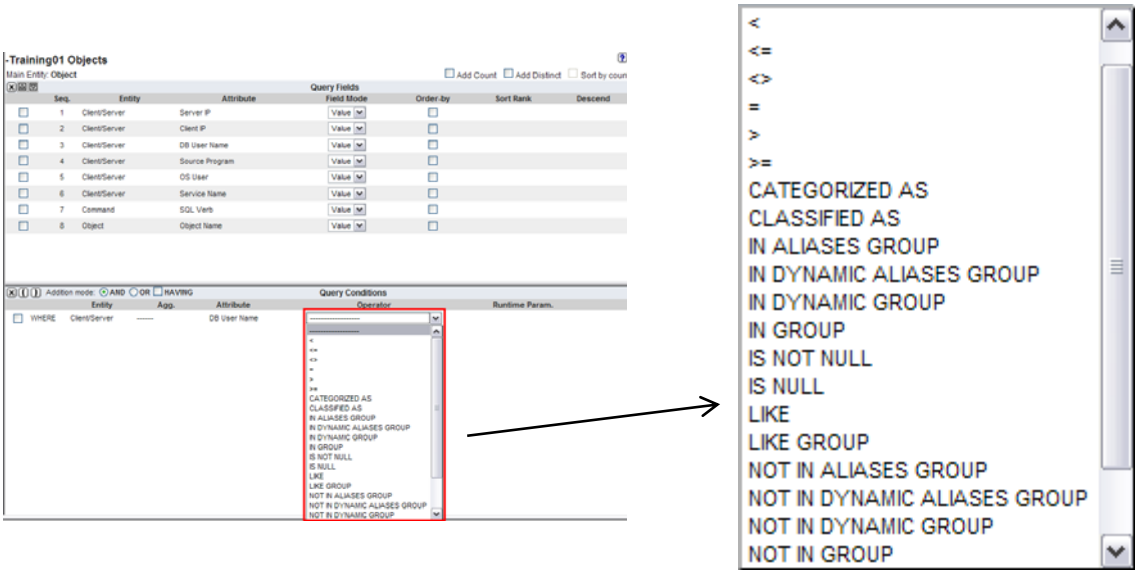
Notes:

The next pages will go into further detail on query conditions and we will use an object-based query as a demonstration. To start a new query:

- Go to **Monitor/Audit** > **Build Reports**
- Press the **Track data access** button
- Enter a **Query Name** and choose *Object* as the **Main Entity**
- Press **Next**

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Query conditions (1 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 11-28. Query conditions (1 of 2) GU2022.0

Notes:

Below are definitions of the available query conditions:

- **<** Less than
- **< =** Less than or equal to
- **< >** Not equal to
- **=** Equal to
- **>** Greater than
- **> =**Greater than or equal to
- **CATEGORIZED AS** - Member of a group belonging to the category selected from the drop-down list to the right, which appears when a group operator is selected.
- **CLASSIFIED AS** - Member of a group belonging to the classification selected from the drop-down list to the right, which appears when a group operator is selected.

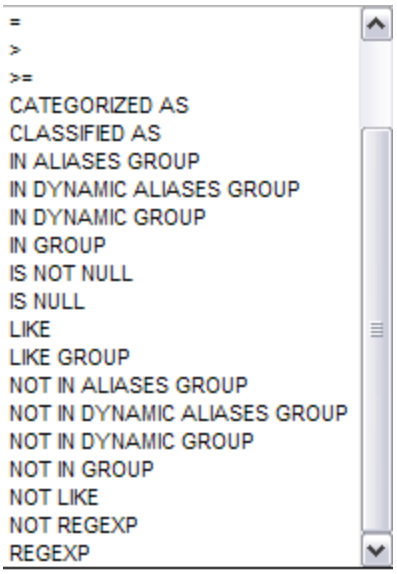
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **IN DYNAMIC GROUP** - Member of a group that will be selected from the drop-down list in the runtime parameter column to the right, which appears when a group operator is selected.
- **IN DYNAMIC ALIASES GROUP** - The operator works on a group of the same type as IN DYNAMIC GROUP, however assumes the members of that group are aliases.
- **IN GROUP** - Member of the group selected from the drop-down list in the runtime parameter column to the right, which appears when a group operator is selected. IN GROUP or IN ALIASES GROUP can not both be used at the same time.
- **IN ALIASES GROUP** - The operator works on a group of the same type as IN GROUP, however assumes the members of that group are aliases. Note that the IN GROUP/IN ALIASES GROUP operators expect the group to contain actual values or aliases respectively. An *alias* provides a synonym that substitutes for a stored value of a specific attribute type. It is commonly used to display a meaningful or user-friendly name for a data value. For example, Financial Server might be defined as an alias for IP address 192.168.2.18.

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Query conditions (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 11-29. Query conditions (2 of 2) GU2022.0

Notes:

Query conditions, continued

- **IS NOT NULL** - Attribute value exists, but may be blank or unprintable
- **IS NULL** - Empty attribute
- **IN PERIOD** - For a timestamp only, is within the selected time period
- **LIKE** -Matches a *like* value specified in the boxes to the right. A like value uses the percent sign as a wildcard character, and matches all or part of the value. Alphabetic characters are not case sensitive. For example, %tea% would match tea, TeA, tEam, steam. If no percent signs are included, the comparison operation will be an equality operation (=).
- **LIKE GROUP** - Matches any member of a group that may contain wildcard member names. For example, if the group contained a member named %tea%, it would match tea, TeA, tEam, steam, etc.

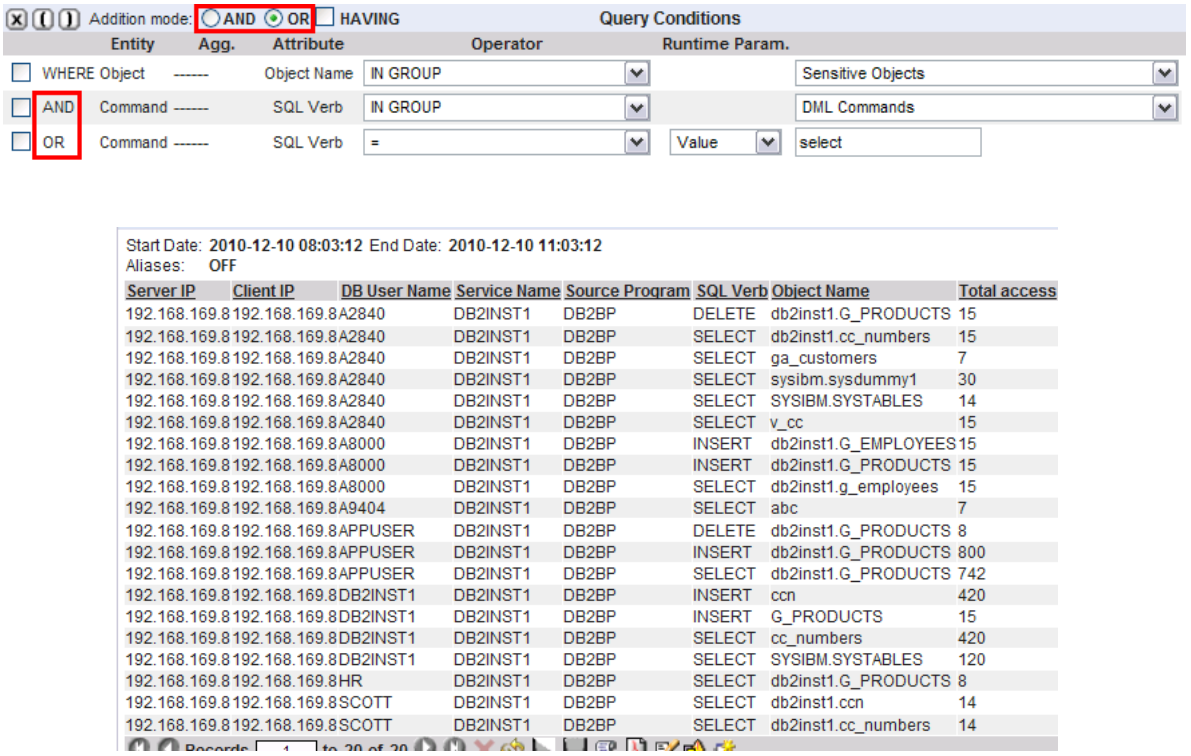
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **NOT IN DYNAMIC GROUP** - Not equal to any member of a group, selected from the drop-down list in the runtime parameter column to the right, which appears when a group operator is selected.
- **NOT IN DYNAMIC ALIASES GROUP** - The operator works on a group of the same type as NOT IN DYNAMIC GROUP, however assumes the members of that group are aliases.
- **NOT IN GROUP** - Not equal to any member of the specified group, selected from the drop-down list in the runtime parameter column to the right, which appears when a group operator is selected.
- **NOT IN ALIASES GROUP** - The operator works on a group of the same type as NOT IN GROUP, however assumes the members of that group are aliases.
- **NOT IN PERIOD** - For a timestamp only, not within the selected time period
- **NOT LIKE** - Not like the specified value (see the description of LIKE, above)
- **NOT REGEXP-** Not matched by the specified regular expression
- **REGEXP** - Matched by the specified regular expression. The Guardium implementation of regular expressions conforms with POSIX 1003.2. The specification can be viewed from: http://www.unix.org/version3/ieee_std.html.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Addition mode: AND/OR


Addition mode: AND HAVING
Query Conditions
Entity
Agg.
Attribute
Operator
Runtime Param.
WHERE Object ------ Object Name IN GROUP Sensitive Objects
AND Command ------ SQL Verb IN GROUP DML Commands
OR Command ------ SQL Verb = Value select
Start Date: 2010-12-10 08:03:12 End Date: 2010-12-10 11:03:12
Aliases: OFF
Server IP | Client IP | DB User Name | Service Name | Source Program | SQL Verb | Object Name | Total access
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | DELETE | db2inst1.G_PRODUCTS | 15
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | SELECT | db2inst1.cc_numbers | 15
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | SELECT | ga_customers | 7
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | SELECT | sysibm.sysdummy1 | 30
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | SELECT | SYSIBM.SYSTABLES | 14
192.168.169.8 | 192.168.169.8 | A2840 | DB2INST1 | DB2BP | SELECT | v_cc | 15
192.168.169.8 | 192.168.169.8 | A8000 | DB2INST1 | DB2BP | INSERT | db2inst1.G_EMPLOYEES | 15
192.168.169.8 | 192.168.169.8 | A8000 | DB2INST1 | DB2BP | INSERT | db2inst1.G_PRODUCTS | 15
192.168.169.8 | 192.168.169.8 | A8000 | DB2INST1 | DB2BP | SELECT | db2inst1.g_employees | 15
192.168.169.8 | 192.168.169.8 | A9404 | DB2INST1 | DB2BP | SELECT | abc | 7
192.168.169.8 | 192.168.169.8 | APPUSER | DB2INST1 | DB2BP | DELETE | db2inst1.G_PRODUCTS | 8
192.168.169.8 | 192.168.169.8 | APPUSER | DB2INST1 | DB2BP | INSERT | db2inst1.G_PRODUCTS | 800
192.168.169.8 | 192.168.169.8 | APPUSER | DB2INST1 | DB2BP | SELECT | db2inst1.G_PRODUCTS | 742
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | INSERT | ccn | 420
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | INSERT | G_PRODUCTS | 15
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | SELECT | cc_numbers | 420
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | SELECT | SYSIBM.SYSTABLES | 120
192.168.169.8 | 192.168.169.8 | HR | DB2INST1 | DB2BP | SELECT | db2inst1.G_PRODUCTS | 8
192.168.169.8 | 192.168.169.8 | SCOTT | DB2INST1 | DB2BP | SELECT | db2inst1.ccn | 14
192.168.169.8 | 192.168.169.8 | SCOTT | DB2INST1 | DB2BP | SELECT | db2inst1.cc_numbers | 14

© Copyright IBM Corporation 2011, 2013

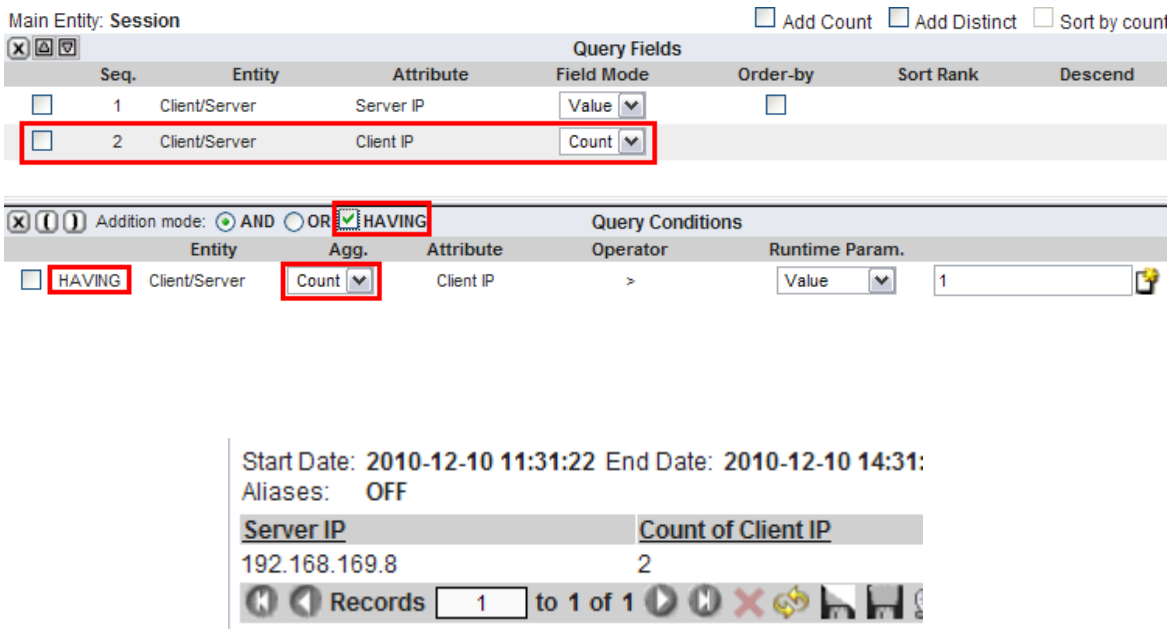
Figure 11-30. Addition mode: AND/OR GU2022.0

Notes:

The **AND** & **OR** radio buttons allow you to control how the conditions are added to the query.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Having



© Copyright IBM Corporation 2011, 2013

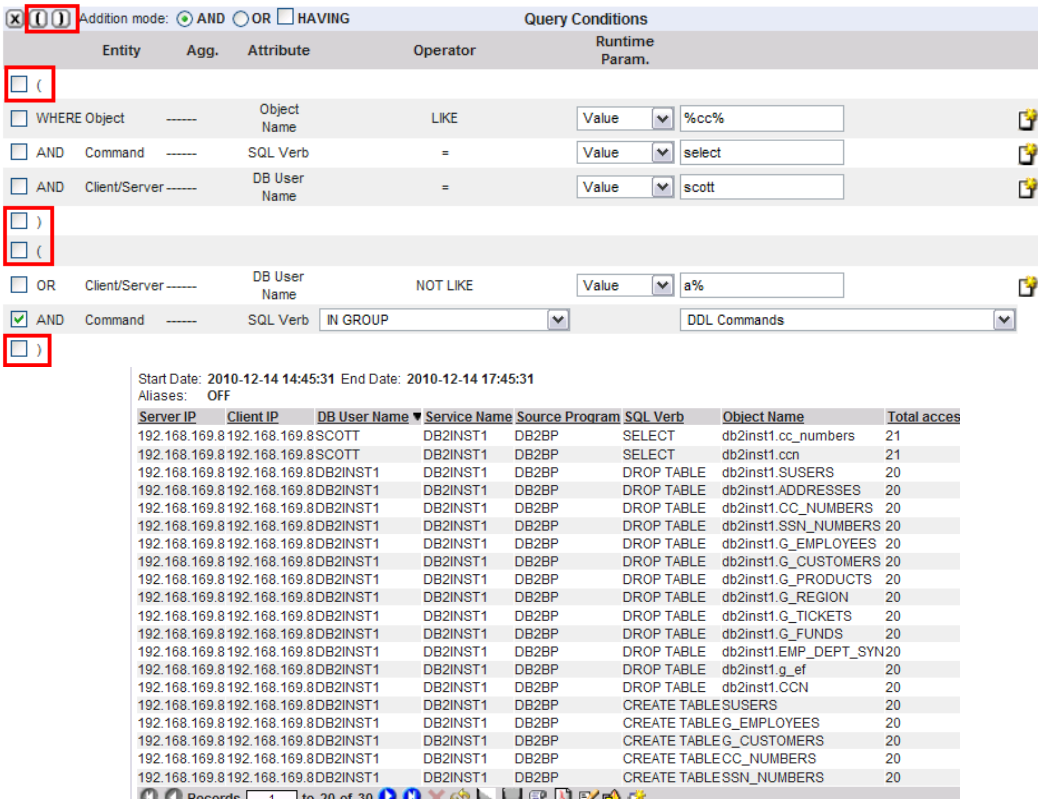
Figure 11-31. Having GU2022.0

Notes:

Having provides the ability to query against aggregate values.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Parenthesis


Addition mode: AND OR HAVING
Query Conditions
Entity
Agg.
Attribute
Operator
Runtime Param.
WHERE Object ------ Object Name LIKE Value %cc%
AND Command ------ SQL Verb = Value select
AND Client/Server ------ DB User Name = Value scott
OR Client/Server ------ DB User Name NOT LIKE Value a%
AND Command ------ SQL Verb IN GROUP DDL Commands
Start Date: 2010-12-14 14:45:31 End Date: 2010-12-14 17:45:31
Aliases: OFF
Server IP | Client IP | DB User Name | Service Name | Source Program | SQL Verb | Object Name | Total acces
192.168.169.8 | 192.168.169.8 | SCOTT | DB2INST1 | DB2BP | SELECT | db2inst1.cc_numbers | 21
192.168.169.8 | 192.168.169.8 | SCOTT | DB2INST1 | DB2BP | SELECT | db2inst1.ccn | 21
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.SUSERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.ADDRESSES | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.CC_NUMBERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.SSN_NUMBERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_EMPLOYEES | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_CUSTOMERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_PRODUCTS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_REGION | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_TICKETS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.G_FUNDS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.EMP_DEPT_SYN | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.g_ef | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | DROP TABLE | db2inst1.CCN | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | CREATE TABLE | SUSERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | CREATE TABLE | G_EMPLOYEES | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | CREATE TABLE | G_CUSTOMERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | CREATE TABLE | CC_NUMBERS | 20
192.168.169.8 | 192.168.169.8 | DB2INST1 | DB2INST1 | DB2BP | CREATE TABLE | SSN_NUMBERS | 20

© Copyright IBM Corporation 2011, 2013

Figure 11-32. Parenthesis GU2022.0

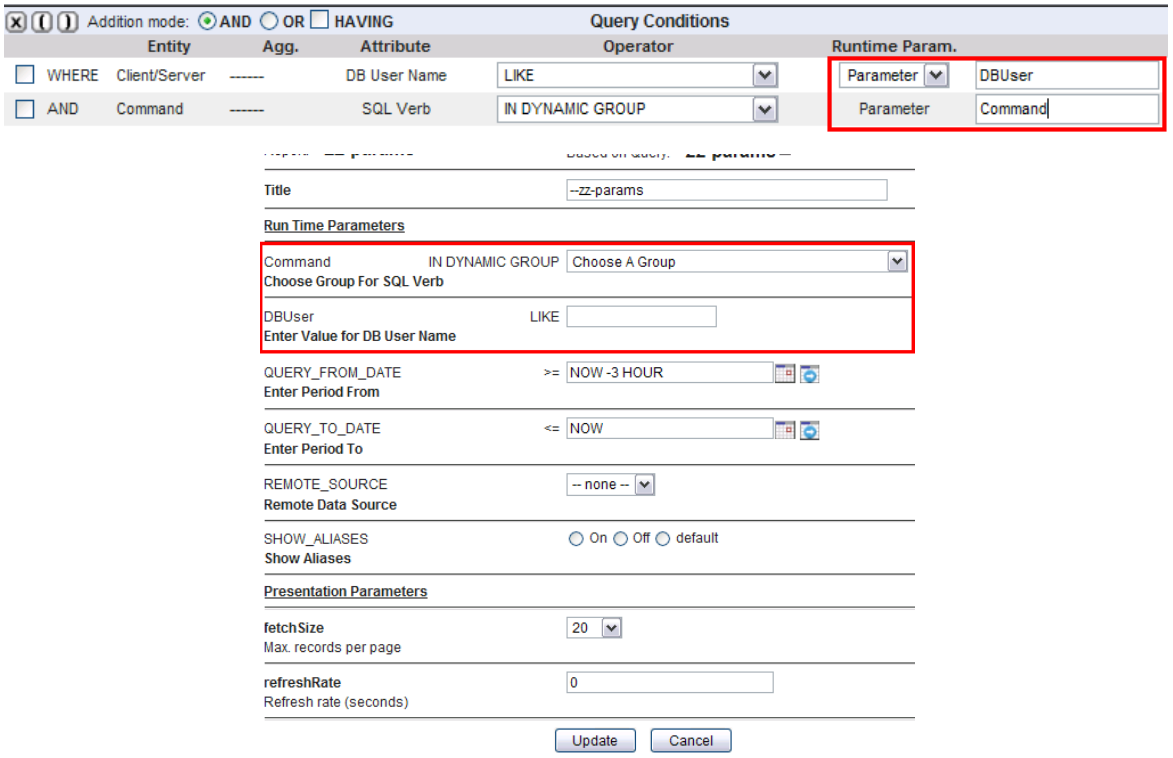
Notes:

The parenthesis buttons provide the ability to add parenthesis button to the query, allowing for complex queries.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Run Time Parameters / Dynamic groups



© Copyright IBM Corporation 2011, 2013

Figure 11-33. Run Time Parameters / Dynamic groups GU2022.0

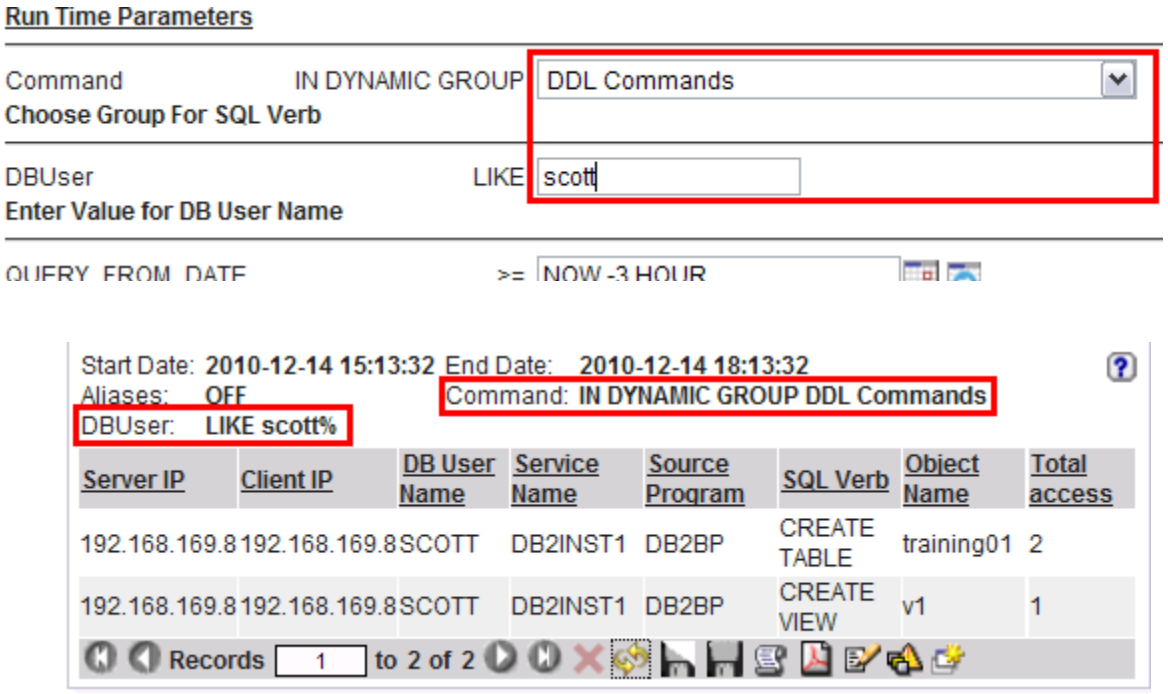
Notes:

Runtime parameters and dynamic groups allow you to supply query conditions each time you run the report. Choose parameter in the **Runtime Param.** column to create a parameter based on a single value. Generally, you should use **LIKE** as your operator when creating runtime parameters. Instead of entering a value in the query field, you will be entering the name of the parameter. In the example above, DBUser is the name of the parameter.

To create a runtime parameter based on group membership, choose **IN DYNAMIC GROUP** as the operator and enter the name of the parameter. In this example Command is the name of the parameter.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Run Time Parameters / Dynamic groups: Results



© Copyright IBM Corporation 2011, 2013

Figure 11-34. Run Time Parameters / Dynamic groups: Results GU2022.0

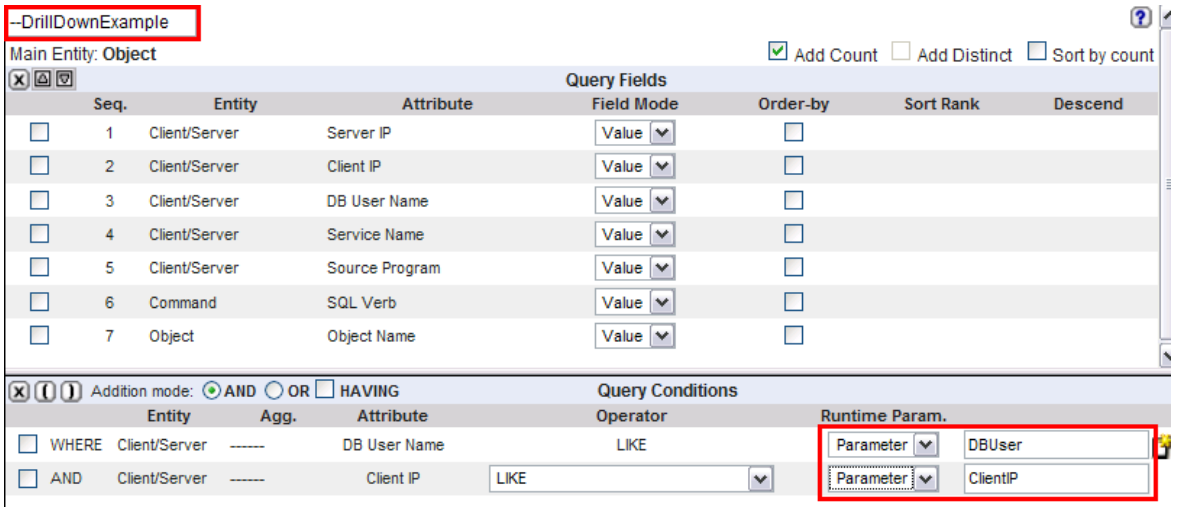
Notes:

The example above demonstrate how runtime parameters work. You simply enter the values in which you are interested and the report will return only data related to those values. Alternatively, you may enter a wildcard (%) to return all data. For dynamic groups, you must choose a value from the pull-down list.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Drill-down reports


--DrillDownExample
Main Entity: Object
Add Count
Add Distinct
Sort by count
Query Fields
Seq. Entity Attribute Field Mode Order-by Sort Rank Descend
1 Client/Server Server IP Value
2 Client/Server Client IP Value
3 Client/Server DB User Name Value
4 Client/Server Service Name Value
5 Client/Server Source Program Value
6 Command SQL Verb Value
7 Object Object Name Value
Addition mode: AND OR HAVING
Query Conditions
Entity Agg. Attribute Operator Runtime Param.
WHERE Client/Server ------ DB User Name LIKE Parameter DBUser
AND Client/Server ------ Client IP LIKE Parameter ClientIP

© Copyright IBM Corporation 2011, 2013

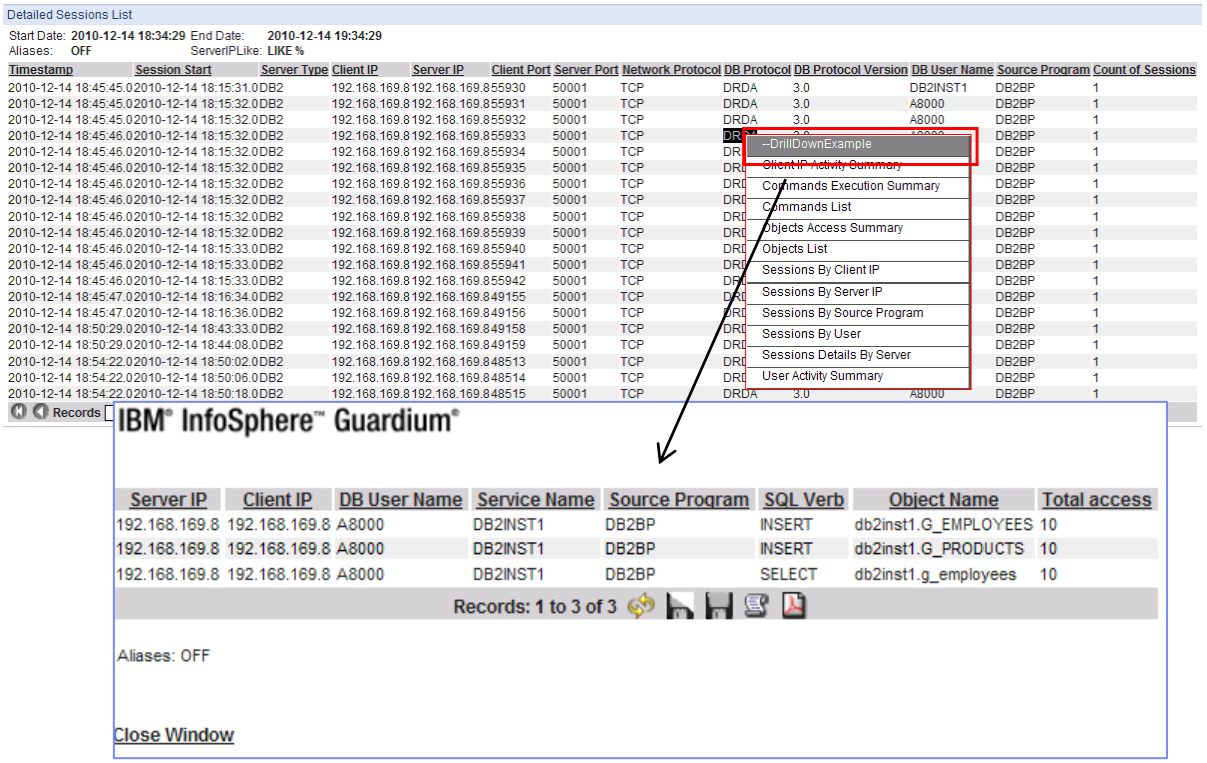
Figure 11-35. Drill-down reports GU2022.0

Notes:

Adding runtime parameters to reports also make them available as drill-down reports. In the example above, there are runtime parameters for database username and client IP. This means that any report containing these two fields will have this report available as a drill down report, as shown on the following page.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Drill-down report example



© Copyright IBM Corporation 2011, 2013

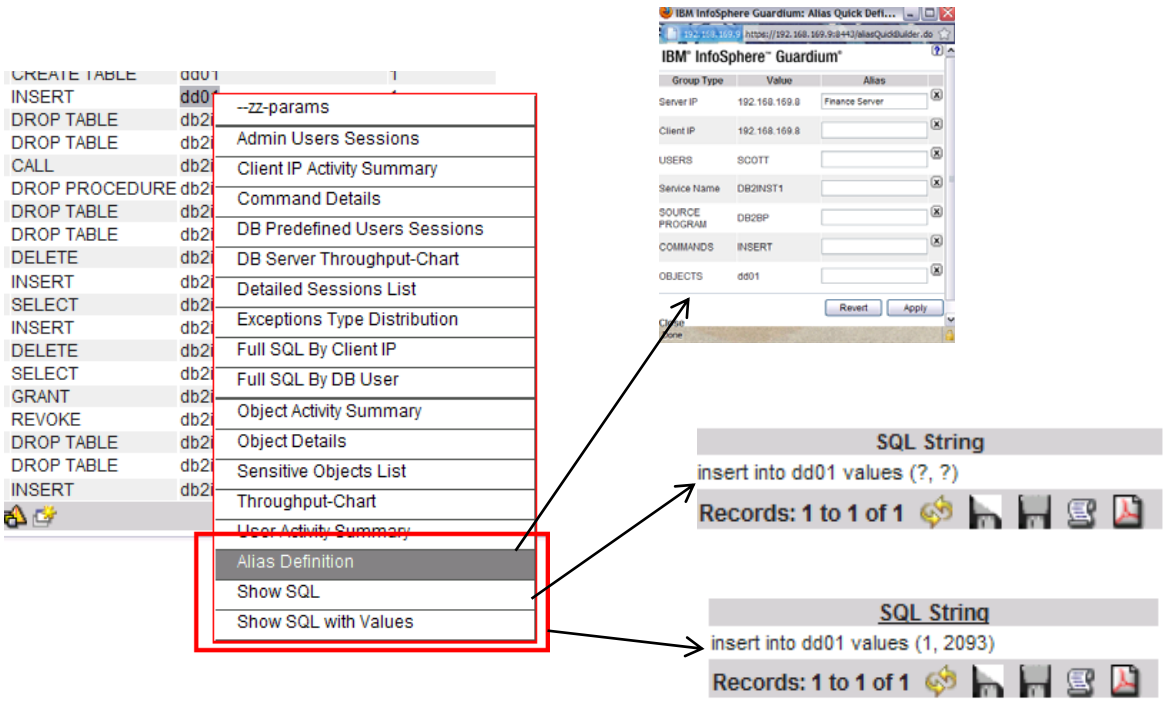
Figure 11-36. Drill-down report example GU2022.0

Notes:

The build-in *Details Sessions List* report contains DB User Name and Client IP as fields, so the new report we created on the previous page is now available as drill down (drill-down reports are invoked by double clicking a row on a report). When you choose a drill down, it simply feeds data from the row that you click to the runtime parameters and displays the result.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Special drill-down options



© Copyright IBM Corporation 2011, 2013

Figure 11-37. Special drill-down options GU2022.0

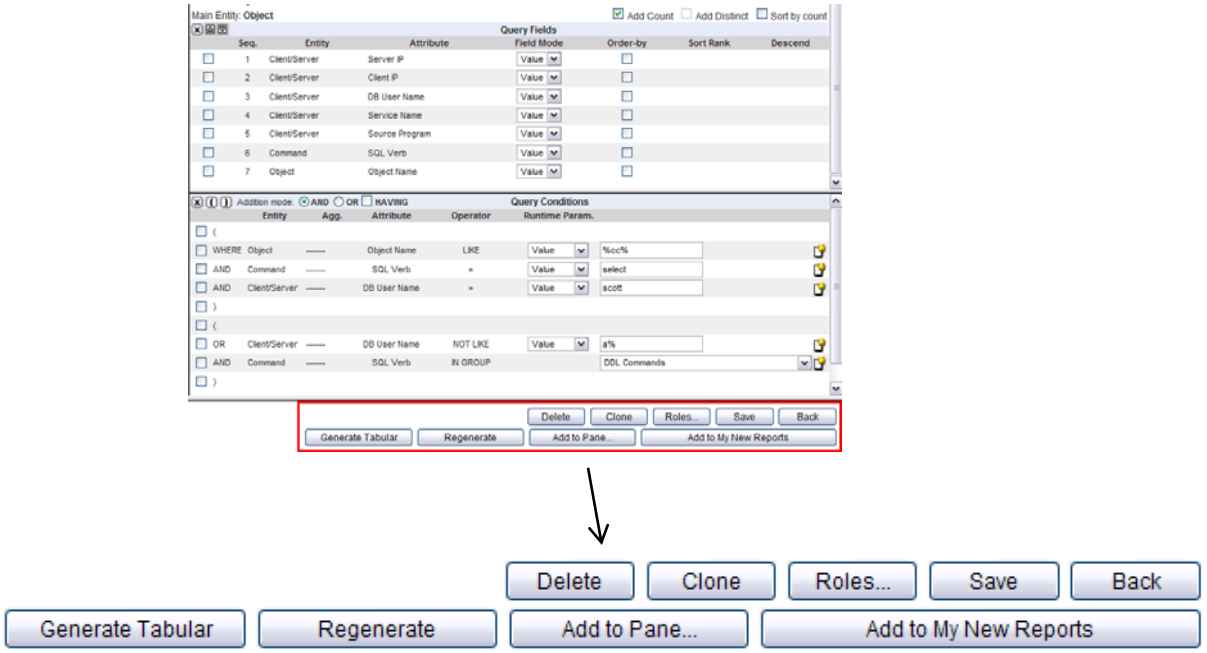
Notes:

In addition to the drilldown reports described on the previous pages, most reports will also display three drill downs with special characteristics:

- **Alias Definition**- When aliases are enabled, this drilldown will bring up a window to apply aliases to the values displayed on the given row
- **Show SQL** – Clicking this option will provide the underlying masked SLQ string for the row selected
- **Show SQL with Values** – This option will display the full unmasked SLQ string, if the request was logged with 'Full Details'

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Query buttons



© Copyright IBM Corporation 2011, 2013

Figure 11-38. Query buttons GU2022.0

Notes:

After adding your required query fields and defining the query conditions you will need to save the query and configure it as a report. As described earlier, the simplest method to do this is to press **Save** and **Add to Pane…** which will save the query, create a tabular report and it to a pane. Other options include:

- **Delete** – Deletes the query. If you have created a report based on the query, you will need to delete the report first.
- **Clone** – Saves the query with a new name.
- **Roles…** - Share the query with other roles.
- **Back** – Exit the query builder without saving your changes.
- **Generate Tabular** - Generates a tabular report without adding it to a pane.
- **Regenerate** – Regenerates the report pane. You should press this button anytime that you add, remove or alter runtime parameters on existing reports.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Add to My New Reports** - Generates a tabular report and adds it to the *My New Reports* pane.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Add conditions to queries
- Use AND and OR clauses
- Use parentheses in queries
- Add a query to a pane
- Create custom run-time parameters

© Copyright IBM Corporation 2011, 2013

Figure 11-39. Topic summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint (1 of 2)

1. Which of the following is NOT a valid conditional operator in Guardium?
   a. REGEXP
   b. IN GROUP
   c. NOT IN GROUP
   d. All of these are valid operators
2. True or false: To add a second condition to a query, you would first select the entity and drop it in the condition frame, and then select either AND or OR.
3. True or false: The HAVING option is only available when the SELECT clause includes one or more aggregate values (such as COUNT, AVG, and so on).

© Copyright IBM Corporation 2011, 2013

Figure 11-40. Checkpoint (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. Which of the following is NOT a valid conditional operator in Guardium?
   a. REGEXP
   b. IN GROUP
   c. NOT IN GROUP
   d. **All of these are valid operators**
2. True or **false**: To add a second condition to a query, you would first select the entity and drop it in the condition frame, and then select either AND or OR.
3. **True** or false: The HAVING option is only available when the SELECT clause includes one or more aggregate values (such as COUNT, AVG, and so on).

Additional information —

Transition statement —

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Checkpoint (2 of 2)

4. How can you supply runtime values to a query?
   a. By using Run Time Parameters
   b. By using Dynamic Groups
   c. Both a and b
   d. Neither a nor b
5. The character used as a wildcard in Guardium queries is:
   a. *
   b. %
   c. ^
   d. _
6. True or false: Adding runtime parameters to reports enables drill-down reports as well.

© Copyright IBM Corporation 2011, 2013

Figure 11-41. Checkpoint (2 of 2) GU2022.0

Notes:

Write your answers here:

4.

5.

6.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

4. How can you supply runtime values to a query?
   a. By using Run Time Parameters
   b. By using Dynamic Groups
   c. **Both a and b**
   d. Neither a nor b&escape_backslash;t
5. The character used as a wildcard in Guardium queries is:
   a. *
   b. %
   c. ^
   d. _
6. **True** or false: Adding runtime parameters to reports enables drill-down reports as well.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 11** in the Exercise Guide. Alternately, you can wait and do Exercises 10, 11, and 12 at the end of this unit.

© Copyright IBM Corporation 2011, 2013

Figure 11-42. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (1 of 2)

1. Which of the following is NOT a valid conditional operator in Guardium?
   a. REGEXP
   b. IN GROUP
   c. NOT IN GROUP
   d. All of these are valid operators
2. True or **false**: To add a second condition to a query, you would first select the entity and drop it in the condition frame, and then select either AND or OR.
3. **True** or false: The HAVING option is only available when the SELECT clause includes one or more aggregate values (such as COUNT, AVG, and so on).

© Copyright IBM Corporation 2011, 2013

Figure 11-43. Checkpoint solutions (1 of 2) GU2022.0

Notes:

Write your answers here:

1.

2.

3.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions (2 of 2)

4. How can you supply runtime values to a query?
   a. By using Run Time Parameters
   b. By using Dynamic Groups
   c. Both a and b
   d. Neither a nor b
5. The character used as a wildcard in Guardium queries is:
   a. *
   b. %
   c. ^
   d. _
6. **True** or false: Adding runtime parameters to reports enables drill-down reports as well.

© Copyright IBM Corporation 2011, 2013

Figure 11-44. Checkpoint solutions (2 of 2) GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

11.3. Report Builder

Instructor topic introduction

What students will do —

How students will do it —

What students will learn —

How this will help students on their job —

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Report builder

After completing this topic, you should be able to:

- Understand the report builder
- Modify reports

© Copyright IBM Corporation 2010, 2013

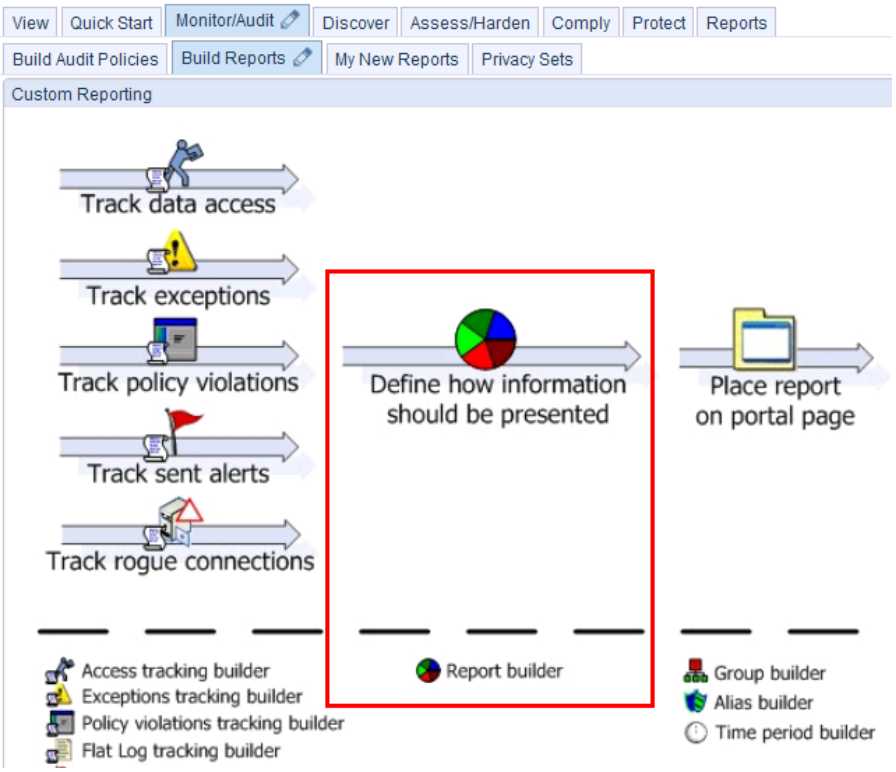
Figure 11-45. Report builder GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Report builder



© Copyright IBM Corporation 2011, 2013

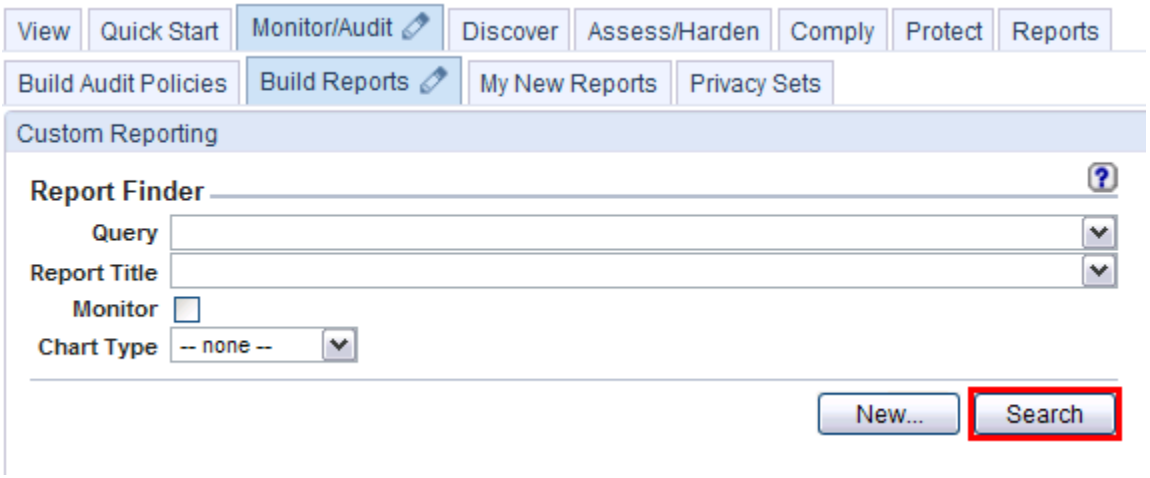
Figure 11-46. Report builder GU2022.0

Notes:

The previous sections focused on the queries that underlie the reports that you view. To modify the actual reports go to **Monitor/Audit** > **Build Report** and click on **Report builder** (**Define how information should be presented**).

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Searching for a report



© Copyright IBM Corporation 2011, 2013

Figure 11-47. Searching for a report GU2022.0

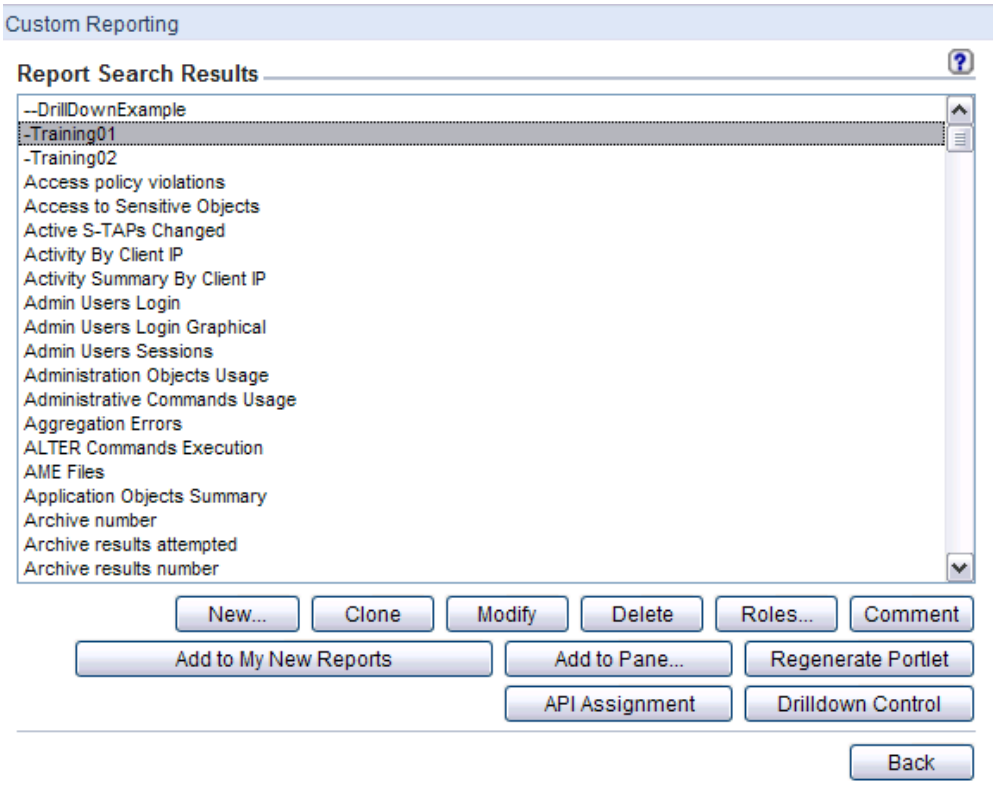
Notes:

To find a specific report you can select its name from *Query* or *Report Title* pull-down menus and press **Search**. Or simply press **Search** with no parameters to return all reports.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Report builder buttons



© Copyright IBM Corporation 2011, 2013

Figure 11-48. Report builder buttons GU2022.0

Notes:

The **Report Search Results** page will display all of the reports found based on your search criteria. Because we left the criteria blank on the previous screen, all reports are presented. Below are the options available from this screen.

- **New**– Create a new report based on previously created query.
- **Clone** – Copy an existing report and save with a new name
- **Modify** – Make changes to an existing report (see the following slides)
- **Delete** – Delete a report. This does not delete the associated query but you must delete the report before you can delete any associated queries.
- **Roles…** – Grant access to the report other users based on their roles. To grant access to a report you must grant the roles to the underlying query first.
- **Comment** - Make notes on a report for reference
- **Add to My New Reports** – Publish the report to the *My New Reports* tab
- **Add to Pane…** - Publish the report to any menu pane

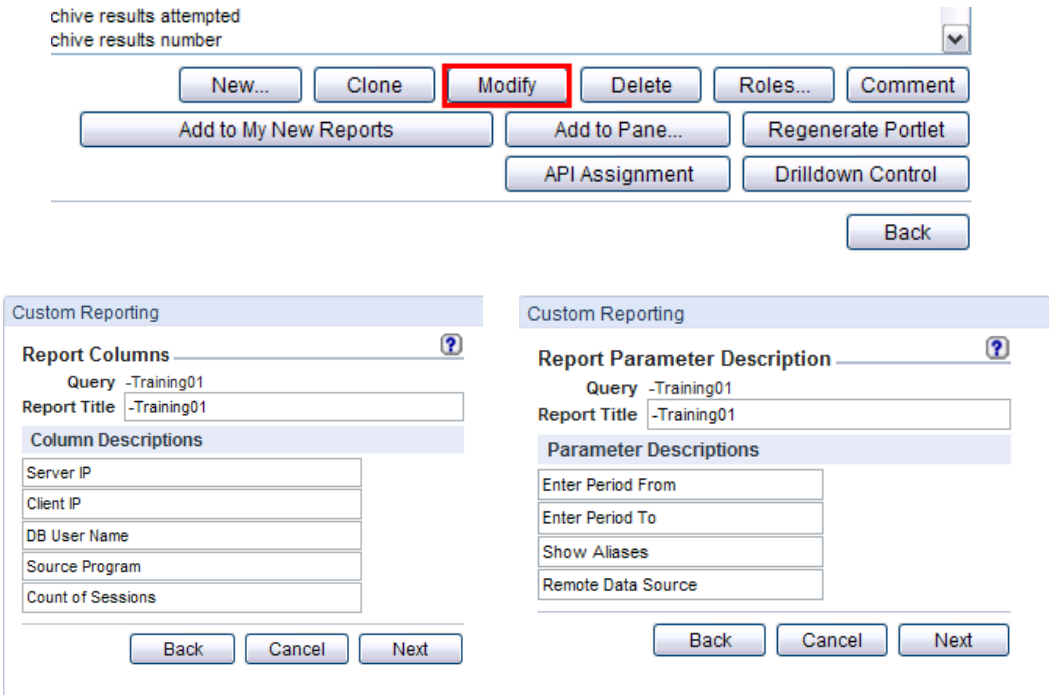
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Regenerate Portlet** - Click this button after changing the runtime parameters for the query on which the report is based
- **API Assignment -** Link additional API functions to predefined Guardium reports or custom reports
- **Drilldown Control** – Remove drilldown entries for this report
- **Back** – Exit the window without making any changes

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Modify report: Tabular (1 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 11-49. Modify report: Tabular (1 of 2) GU2022.0

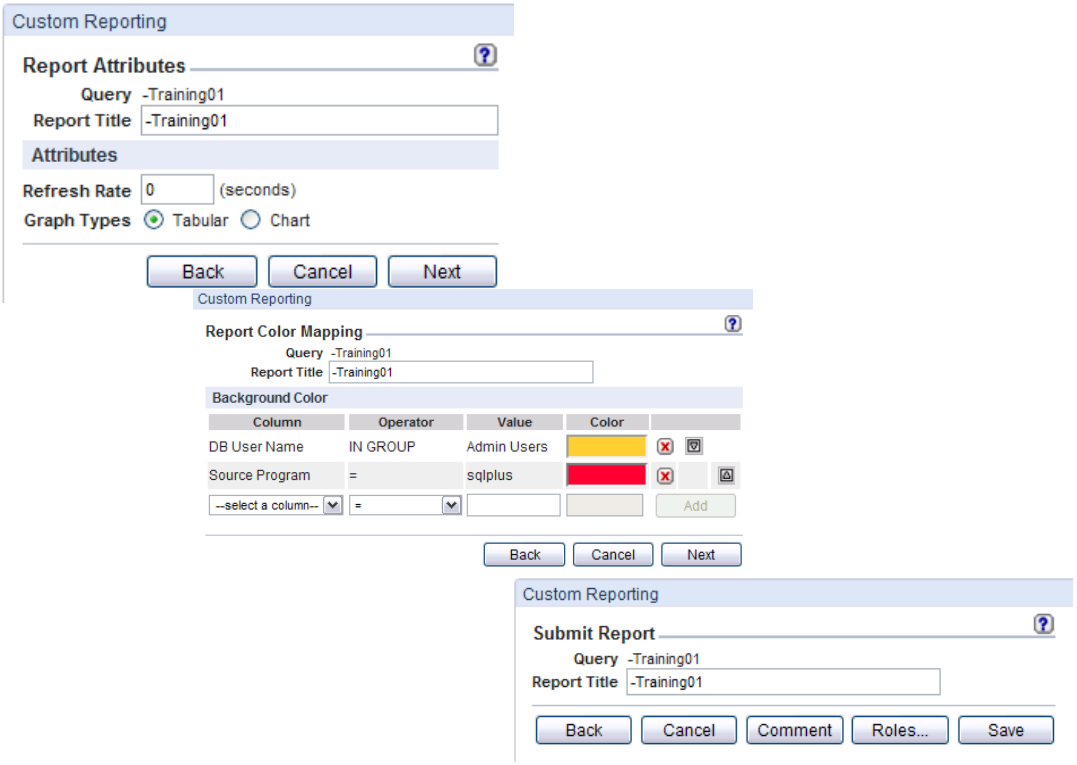
Notes:

To make changes to report click the **Modify** button, which will present a series of windows to change all of the report's settings.

- **Report Columns** – Changes the column names
- **Report Parameter Description** – Changes the description of the run time parameters

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Modify report: Tabular (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 11-50. Modify report: Tabular (2 of 2) GU2022.0

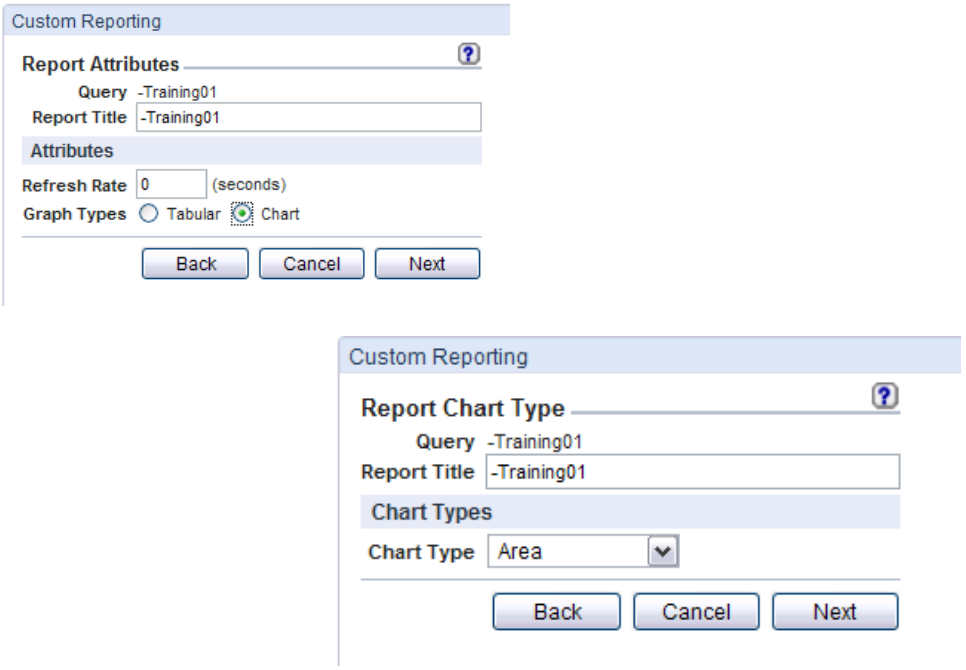
Notes:

- **Report Attributes** – Changes the report title and default refresh rate. This screen also allows you to change the report from a tabular report to a chart.
- **Report Color Mapping**– Allows you to color code report rows based on a field value or group membership.
- **Submit Report** – Saves any changes made.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Modify report: Chart (1 of 2)



© Copyright IBM Corporation 2011, 2013

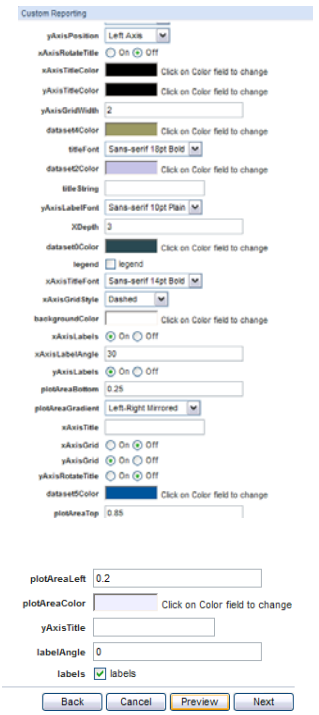
Figure 11-51. Modify report: Chart (1 of 2) GU2022.0

Notes:

When choosing **Chart** instead of tabular on the Reports Attributes window, the next window will prompt you to select a **Report Chart Type**. On the Chart Type pull-down menu, choose from standard chart types, such as Area, Line, Pie, etc.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Modify report: Chart (2 of 2)



© Copyright IBM Corporation 2011, 2013

Figure 11-52. Modify report: Chart (2 of 2) GU2022.0

Notes:

The final screen allows you to change the chart formatting.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Topic summary

Having completed this topic, you should be able to:

- Understand the report builder
- Modify reports

© Copyright IBM Corporation 2011, 2013

Figure 11-53. Topic summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. True or false: A query needs a report and a report needs a query.
2. What format(s) are available for Guardium reports?
    1. Tabular
    2. Chart
    3. Both a and b
    4. Neither a nor b

© Copyright IBM Corporation 2011, 2013

Figure 11-54. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. **True** or false: A query needs a report and a report needs a query.
2. What format(s) are available for Guardium reports?
   a. Tabular
   b. Chart
   c. **Both a and b**
   d. Neither a nor b

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Transition statement —

Unit summary

Having completed this unit, you should be able to:

- Understand domains, entities, and attributes
- Create custom queries and reports

© Copyright IBM Corporation 2011, 2013

Figure 11-55. Unit summary GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 12** in the Exercise Guide. Alternately, if you waited, you can do Exercises 10, 11, and 12 now.

© Copyright IBM Corporation 2012, 2013

Figure 11-56. Exercise GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. **True** or false: A query needs a report and a report needs a query.
2. What format(s) are available for Guardium reports?
    1. Tabular
    2. Chart
    3. **Both a and b**
    4. Neither a nor b

© Copyright IBM Corporation 2011, 2013

Figure 11-57. Checkpoint solutions GU2022.0

Notes:

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit 12. Compliance Workflow Automation

Estimated time

00:30

What this unit is about

This unit describes how to automate audit activities into a compliance workflow.

What you should be able to do

After completing this unit, you should be able to:

- Understand how to consolidate and automate audit activities into a compliance workflow
- Determine who needs to review the audit results and manage the signoffs
- Establish a schedule for delivery

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit objectives

After completing this unit, you should be able to:

- Understand how to consolidate and automate audit activities into a compliance workflow
- Determine who needs to review the audit results and manage the signoffs
- Establish a schedule for delivery

© Copyright IBM Corporation 2011, 2013

Figure 12-1. Unit objectives GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Compliance Workflow Automation

- Compliance Workflow Automation provides facilities to automate and integrate audit activities into a compliance workflow:
  - Group multiple audit tasks (reports, vulnerability assessments, and so on) into a single process.
  - Schedule the process to run on a regular basis, in background mode.
  - Assign the process to its originator for viewing
  - Assign the process to other users, or to a group of users or a role.
  - Create the requirement that the assignees sign off on the result.
  - Allow users to add comments and notations.
  - Allow escalation of the results.

© Copyright IBM Corporation 2011, 2013

Figure 12-2. Compliance Workflow Automation GU2022.0

Notes:

Guardium's compliance workflow automations provides the ability to transform the management of database security from time-consuming manual activities performed periodically to a continuous, automated process that supports company privacy and governance requirements, such as PCI-DSS, SOX, Data Privacy and HIPAA. It includes the capabilities to:

- Streamline the compliance workflow process by consolidating, in one spot, database activity monitoring tasks, including asset discovery, vulnerability assessment and hardening reports, and database audit reports.
- Distribute reports to a specific list of recipients in a specific order, and optionally require sign-off by key stakeholders.
- Allow recipients to escalate delivery of reports following specified criteria.
- Export audit results to external repositories for additional forensic analysis – Syslog, CSV/CEF files, and/or external feeds.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Compliance Workflow Automation elements

Elements of the compliance workflow automation process include:

- **A distribution plan**
  - Defines receivers, which can be individual users, user groups, or roles.
  - Defines the review/sign responsibility for each receiver.
  - Defines the distribution sequence.
- **A set of tasks**
  - Reports
  - Security assessments
  - Entity audit trails
  - Privacy sets
  - Classification processes
  - External feeds
- **A schedule**
  - The audit process can be run immediately, or a schedule can be defined to run the process on a regular basis.

© Copyright IBM Corporation 2011, 2013

Figure 12-3. Compliance Workflow Automation elements GU2022.0

Notes:

A compliance workflow automation process answers the following questions:

What type of report, assessment, audit trail, or classification is needed?

Who should receive this information and how are signoffs handled?

What is the schedule for delivery?

A workflow process may contain any number of **audit tasks**, including:

- **Reports.** custom or pre-defined. Guardium provides hundreds of predefined reports, with more than 100 regulation-specific reports.
- **Security assessment** report. The security database assessment scans the database infrastructure for vulnerabilities, and provides an evaluation of database and data security health, with both real-time and historical measurements. It compares current environment against preconfigured vulnerability tests based on known flaws and vulnerabilities, grouped using common database security best practices (like STIG and CIG1), as well as incorporating custom tests. The application generates a Security Health Report Card, with weighted metrics (based

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

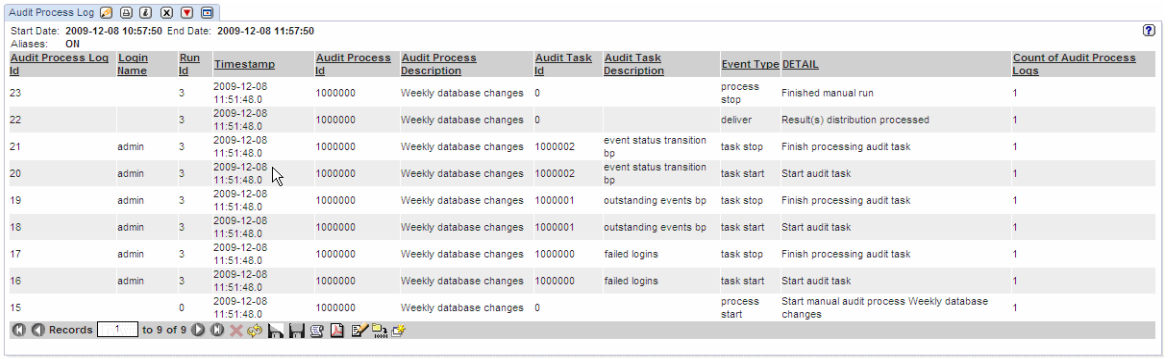
on best practices) and recommends action plans to help strengthen database security.

- An **entity audit trail.** A detailed report of activity relating to a specific entity is produced (for example, a client IP address or a group of addresses).
- A **privacy set.** A report detailing access to a group of object-field pairs (a Social Security number and a date of birth, for example) is produced during a specified time period.
- A **classification** process. The existing database metadata and data is scanned, reporting on information that may be sensitive, such as Social Security numbers or credit card numbers.
- An **external feed**. Data can be exported to an external specialized application for further forensic analysis.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Compliance Workflow Automation log

- Compliance Workflow Automation includes a detailed activity log.



Audit Process Log

Start Date: 2009-12-08 10:57:50 End Date: 2009-12-08 11:57:50
Aliases: ON

Audit Process Log Id	Login Name	Run Id	Timestamp	Audit Process Id	Audit Process Description	Audit Task Id	Audit Task Description	Event Type	DETAIL	Count of Audit Process Logs
23		3	2009-12-08 11:51:48.0	1000000	Weekly database changes	0		process stop	Finished manual run	1
22		3	2009-12-08 11:51:48.0	1000000	Weekly database changes	0		deliver	Result(s) distribution processed	1
21	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000002	event status transition bp	task stop	Finish processing audit task	1
20	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000002	event status transition bp	task start	Start audit task	1
19	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000001	outstanding events bp	task stop	Finish processing audit task	1
18	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000001	outstanding events bp	task start	Start audit task	1
17	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000000	failed logins	task stop	Finish processing audit task	1
16	admin	3	2009-12-08 11:51:48.0	1000000	Weekly database changes	1000000	failed logins	task start	Start audit task	1
15		0	2009-12-08 11:51:48.0	1000000	Weekly database changes	0		process start	Start manual audit process Weekly database changes	1

Records 1 to 9 of 9

© Copyright IBM Corporation 2011, 2013

Figure 12-4. Compliance Workflow Automation log GU2022.0

Notes:

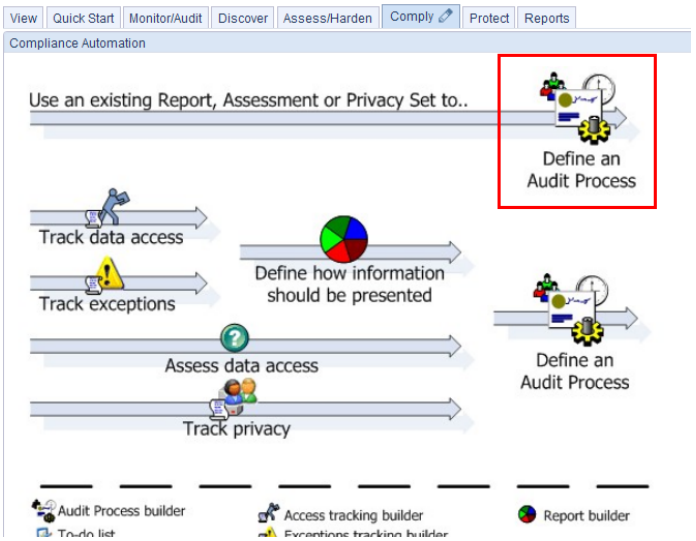
Compliance Workflow Automation maintains a detailed activity log for all tasks, which includes task start and end times. A report, called the Audit Process Log, of information in the activity log is available from the Guardium Monitor tab.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Define an Audit Process

- Defined and maintained by members of the infosec role.
- Available on the Comply pane, under Define an Audit Process.



© Copyright IBM Corporation 2011, 2013

Figure 12-5. Define an Audit Process GU2022.0

Notes:

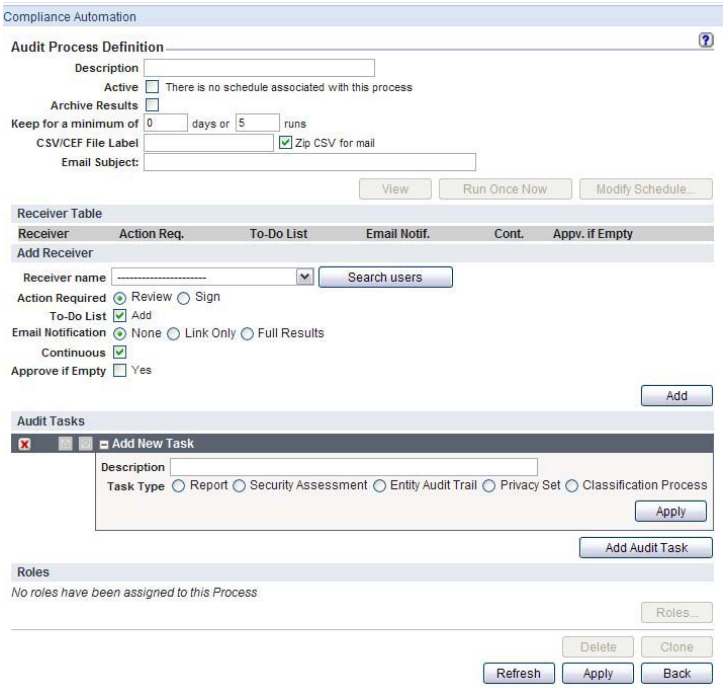
Workflow processes are created and maintained by members of the infosec role.

To create a new workflow (audit) process, go to the **Comply** pane and Select **Define an Audit Process**.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Compliance Automation screen

- A new compliance automation process consists of four parts:
  - Audit Process Definition
  - Receiver Table
  - Audit Tasks
  - Roles/Process Management



© Copyright IBM Corporation 2011, 2013

Figure 12-6. Compliance Automation screen GU2022.0

Notes:

Create a new compliance automation process by selecting NEW from the Define an Audit Process screen. The Compliance Automation screen is composed of four sections:

- Audit Process Definition
- Receiver Table
- Audit Tasks
- Roles/Process Management

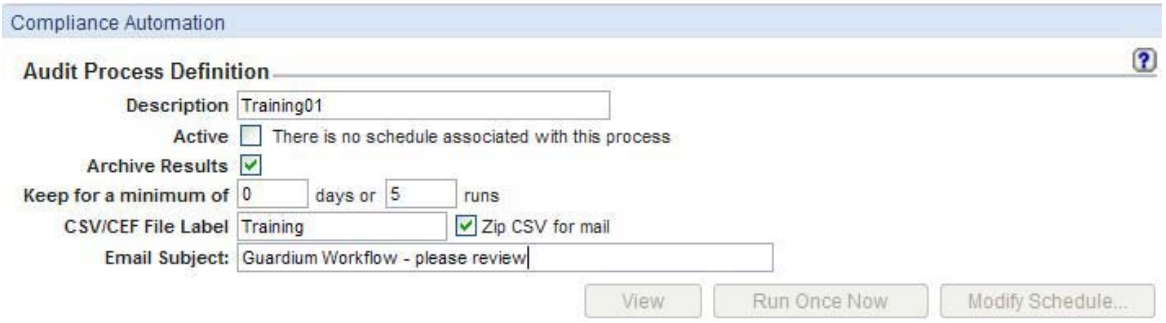
Each section will be discussed on the upcoming pages.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Audit Process Definition

- The Audit Process Definition includes general options for the process:
  - Description
  - Archiving results
  - File label
  - Email subject
  - Activation
  - Minimum retention period
  - Zipping results



© Copyright IBM Corporation 2011, 2013

Figure 12-7. Audit Process Definition GU2022.0

Notes:

The Audit Process Definition menu includes general options for the process, and includes:

- **Description** – Enter a name of the audit process.
- **Active** – Check this box to enable a schedule for the audit process.
- **Archive Results** – Checking this box will include this audit processes' results in the Results Archive process.
- **Keep for a minimum of** *x* ***days*** *x* **runs** – Enter a number in either of this fields to control the purge schedule for this processes results.
- **CSV/CEF Label** - If one or more tasks create CSV or CEF files, you can optionally enter a label to be included in all file names, in the **CSV/CEF File Label** box.
- **Zip CSV for mail** –The CSV file be compressed, or Zipped, by clicking on the Zip for mail box to add a checkmark.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Email Subject** – This is used in the emails for all receivers for that audit process. The subject may contain one (or more) of the following variables that will be replaced at run time for the subject:
  - %%ProcessName will be replaced with the audit process description
  - %%ExecutionStart will be replaced with the start date and time of the first task.
  - %%ExecutionEnd will be replaced with the end date and time of the last task.

It also includes buttons to:

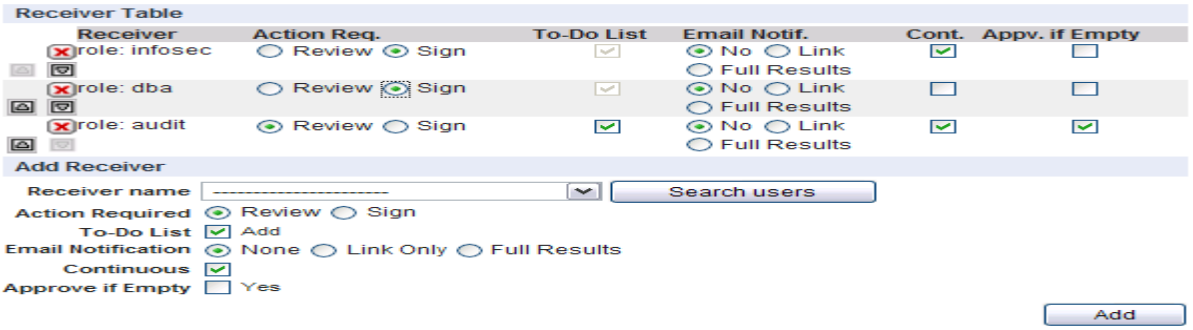
- **View** – After the audit process has been run at least once, this button will allow you view the results.
- **Run Once Now** – Run the audit process on an ad hoc basis. The Receiver Table and Task Definition sections must be completed for this to execute.
- **Modify Schedule** – Create or modify a schedule for the audit process. The Receiver Table and Task Definition sections must be completed and the Active checkbox must be checked to enable scheduled processes.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Receiver Table

- The receiver table controls who receives the reports, and includes:
  - Receiver name - Action receiver must take
  - To Do list notification - Email notification
  - Continuation flag - Empty approval flag



© Copyright IBM Corporation 2011, 2013

Figure 12-8. Receiver Table GU2022.0

Notes:

The receiver table controls who receives the workflow, the order in which users receive it, and the user's required action upon receipt. Options include:

- **Receiver name** - The receiver is selected from a drop-down list of Guardium individual users or roles. If a role is selected, all users with that role will receive the results; however, if signing is required, only one user will need to sign the results.
- **Action Required –** Any actions the receiver is required to take a detailed here. The received may be required to:
  - **Review** - Indicates that the receiver does not need to sign the results.
  - **Sign** - Indicates that the receiver must sign the results (electronically, by clicking the **Sign Results** button when viewing the results online).
- **To-Do List** – A receiver can be notified of the report's delivery via the user's audit process To Do List.
  - **Checked** – Indicates the receiver should be notified through the To Do list.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

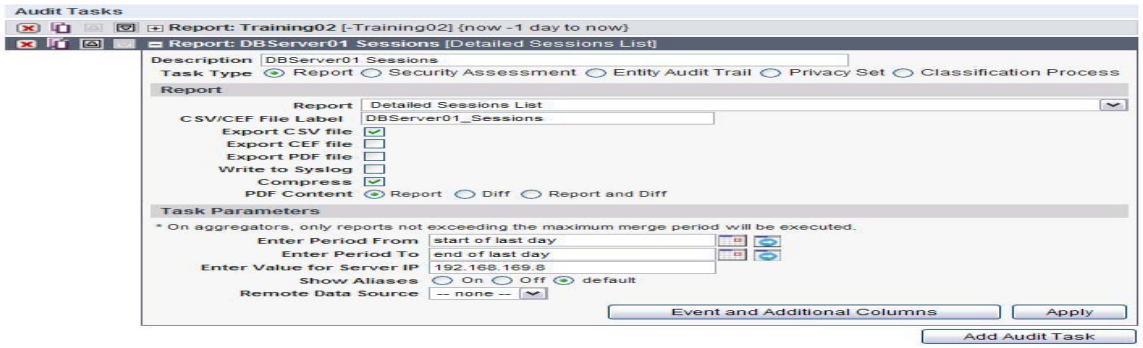
  - **Unchecked** – Indicates the receiver should not be notified through the To Do list.
- **Email Notification –** A receiver can be notified of the report's delivery via email.
  - **None** - E-mail will **not** be sent to the receiver.
  - **Link Only** - E-mail will contain a hypertext link to the results, which can be accessed from the Guardium appliance.
  - **Full Results** - E-mail will contain a copy of the results in PDF or CSV format. Be aware that the results from Classification or Assessment tasks may return sensitive information.
- **Continuous** - The Continuous flag controls whether or not distribution of results continues to the next receiver (the default), or stops until this receiver has taken the appropriate action (**Review** or **Review and Sign**).
  - Checked – If the Continuous box is checked, and the receiver is an individual user, that user must take the indicated action before the results will continue on to the next receiver in the list. If the Continuous box is checked, and the receiver is a group or a role, one member of that group or role must take the indicated action before the results will continue on to the next receiver in the list.
  - Unchecked - If the **Continuous** box is cleared, the results will immediately be released to the next receiver on the list.
- **Approve if Empty -** The Approve if Emtpy flag controls how the distribution of results takes place when the results are empty.
  - **Checked** - When this checkbox is checked, if all the reports of the task are empty, the system will automatically sign the result (and/or mark it as viewed) and continue (if relevant). It will NOT notify the recipient via either the To Do list or email. It will not generate any PDF/CSV/CEF files.
  - **Unchecked** – When this checkbox is unchecked, all normal processing takes place even when the results are empty.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Audit Tasks

- Audit Tasks controls what is delivered to the receivers.
  - Reports
  - Secuirty Assessments
  - Entity Audit Trails
  - Classification Processes


Audit Tasks
Report: Training02 [-Training02] (now -1 day to now)
Report: DBServer01 Sessions [Detailed Sessions List]
Description DBServer01 Sessions
Task Type Report Security Assessment Entity Audit Trail Privacy Set Classification Process
Report
Report Detailed Sessions List
CSV/CEF File Label DBServer01_Sessions
Export CSV file
Export CEF file
Export PDF file
Write to Syslog
Compress
PDF Content Report Diff Report and Diff
Task Parameters
* On aggregators, only reports not exceeding the maximum merge period will be executed.
Enter Period From start of last day
Enter Period To end of last day
Enter Value for Server IP 192.168.169.8
Show Aliases On Off default
Remote Data Source -- none --
Event and Additional Columns
Apply
Add Audit Task

© Copyright IBM Corporation 2011, 2013

Figure 12-9. Audit Tasks GU2022.0

Notes:

The audit tasks section controls what is delivered to the receivers:

- **Description** – Enter a user-defined description of the task.
- **Task Type** – Report, Security Assessment, Entity Audit Trail, Privacy Set, Classification Process. In this example, we will choose a report.
- **Report** – Select the report that you would like to send from the pull-down list.
- **CSV/CEF File Label** - Enter an optional label for the file in the **CSV/CEF File Label** box. The default is from the Description for the task. This label will be one component of the generated file name (another will be the label defined for the workflow automation process).
- **Export CSV file** – Check this box to export the report results to an CSV file. The CSV export process must also be configured from Administration Console.
- **Export CEF file** – Check this box to export the report results to a CEF file.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

- **Export PDF file** – Check to export a PDF file. A PDF file (with similar name as CSV Export file) for this Audit Task is created and exported together with the CSV/CEF files. Note: The Export PDF file will not be compressed, even if the Compress box in the previous step is checked.
- **Write to Syslog** - If Export CEF file was selected, optionally mark the **Write CEF to Syslog** box to write the CEF records to syslog. If the remote syslog facility is enabled, the CEF file records will thus be written to the remote syslog.
- **Compress** - If this box is checked, then the CSV/CEF files to be exported will be compressed.
- **PDF Content** - The selection of PDF Content are: Report (the current results), Diff (difference between one earlier report and a new report) and Reports and Diff (both). Note: The selection of PDF Content applies to both PDF attachments and PDF export files. The Diff result only applies only AFTER the first time this task is run. There is no Diff with a previous result if there is no previous result. The maximum number of rows that can be compared at one time is 5000. If the number of result rows exceeds the maximum, the message "(compare first 5000 rows only)" will show up in the diff result.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Roles/Process Management

- Roles can be
  - Deleted
  - Cloned
  - Refreshed

© Copyright IBM Corporation 2011, 2013

Figure 12-10. Roles/Process Management GU2022.0

Notes:

Press the **Roles…** button to allow access to the audit process definition to other users.

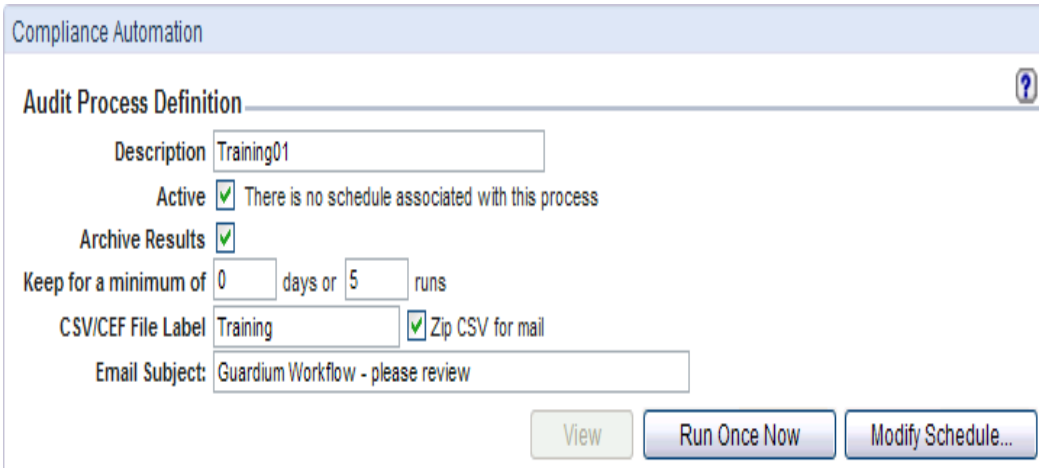
The remaining buttons are used to manage the audit process:

- **Delete**– Deletes the audit process
- **Clone** – Copy the audit process with a new name
- **Add Comments** – Add notes for reference
- **Refresh** – Updates the contents
- **Apply** – Save changes to the audit process
- **Back** – Exit the audit process without saving changes

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Activating and running an audit process

- The audit process can now be activated and either run or scheduled.



© Copyright IBM Corporation 2011, 2013

Figure 12-11. Activating and running an audit process GU2022.0

Notes:

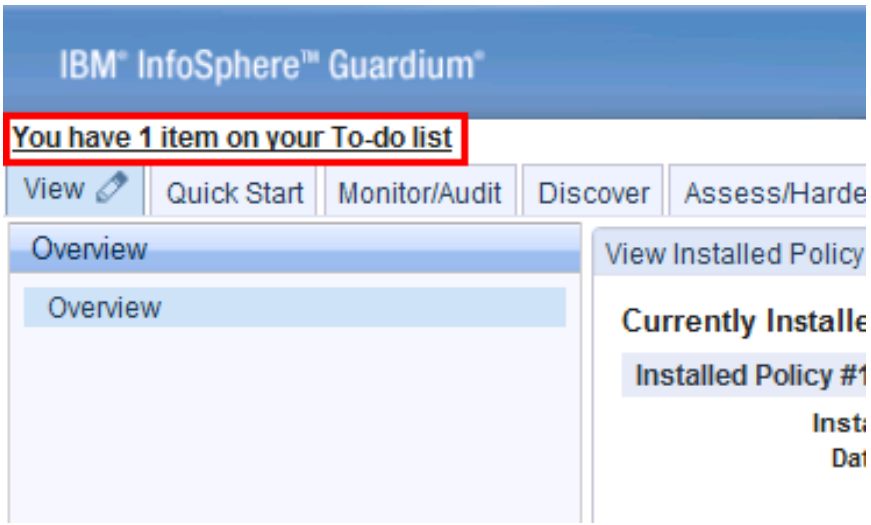
Once the process receivers and tasks are complete, the Audit Process can now be marked as **Active** and scheduled. Also, you could press **Run Once Now** to execute the Audit Process immediately.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

To Do notification

- A user's To Do list includes the number of work items waiting, and a clickable link to those items.



© Copyright IBM Corporation 2011, 2013

Figure 12-12. To Do notification GU2022.0

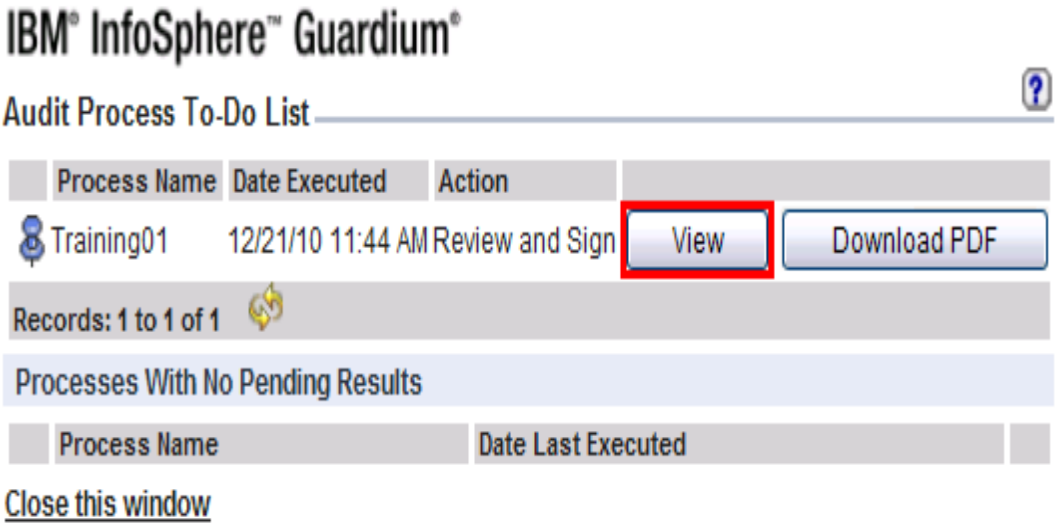
Notes:

After an audit process has be run, receivers will be notified of new results via e-mail or through a link when logging into the appliance. To view an audit process, click on the link then press the **View** button.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Viewing an audit process

- The To Do list may contain multiple items
- View allows you go to to a particular item



© Copyright IBM Corporation 2011, 2013

Figure 12-13. Viewing an audit process GU2022.0

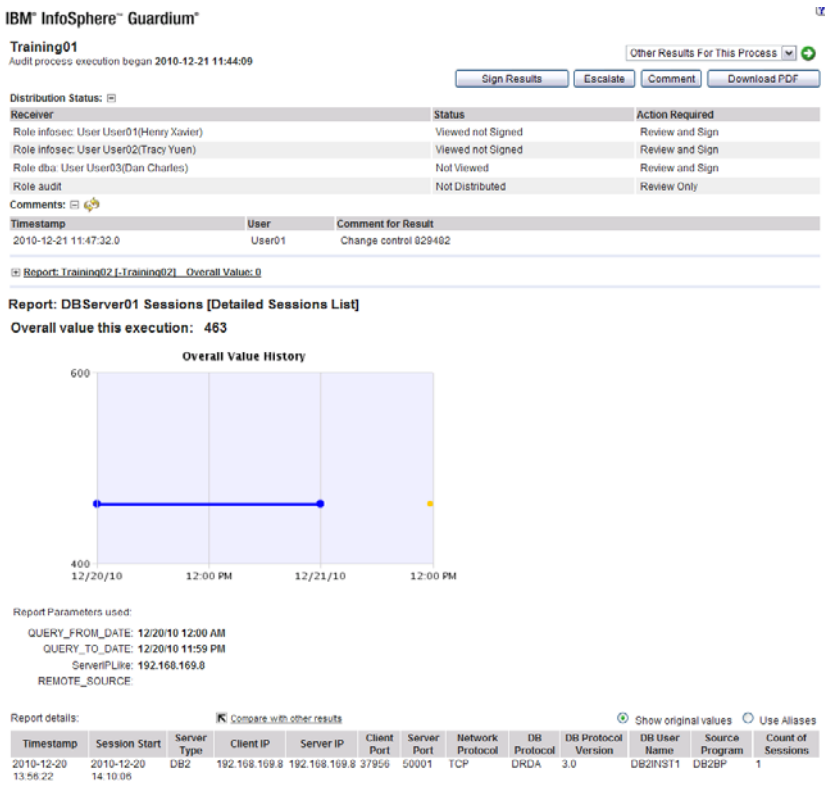
Notes:

After an audit process has be run, receivers will be notified of new results via e-mail or through a link when logging into the appliance. To view an audit process, click on the link then press the **View** button.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Report delivery



© Copyright IBM Corporation 2011, 2013

Figure 12-14. Report delivery GU2022.0

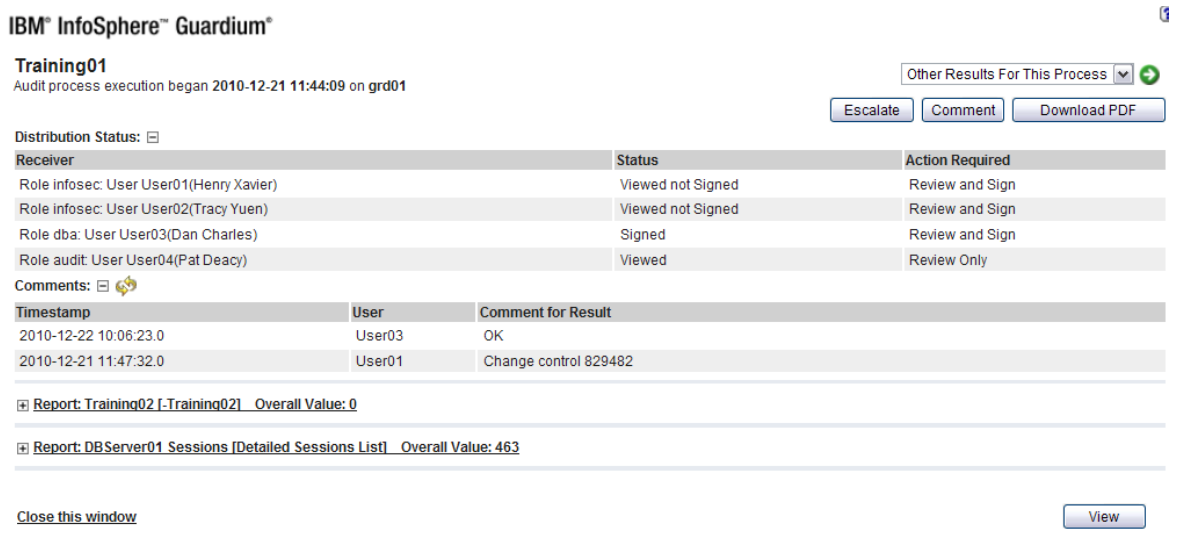
Notes:

The workflow results contain each of the tasks configured and the status of the workflow, including the distribution status and any comments made by other receivers.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Workflow results

- Workflow results include:
  - Distribution Status
  - Comments



© Copyright IBM Corporation 2011, 2013

Figure 12-15. Workflow results GU2022.0

Notes:

This is an example of a completed audit process.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint

1. The three elements of a Compliance Automation Workflow process are a _____, a _____, and a _____.

2. True or false: A user can optionally be notified of pending work in the Compliance Automation Workflow through a To Do list link.

3. The _____ table controls who receives the reports and what action(s) they must take.

4. True or false: A Workflow can be either activated and scheduled to run, or it can be run once now, but not both.

5. Which button takes you to a particular item in your To Do list?
    1. GOTO
    2. VIEW
    3. OPEN
    4. SAVE

© Copyright IBM Corporation 2011, 2013

Figure 12-16. Checkpoint GU2022.0

Notes:

Write your answers here:

1.

2.

3.

4.

5.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Instructor notes:

Purpose —

Details —

Answers

1. The three elements of a Compliance Automation Workflow process are a **distribution plan**, a **set of tasks**, and a **schedule**.
2. **True** or false: A user can optionally be notified of pending work in the Compliance Automation Workflow through a To Do list link.
3. The **receiver** table controls who receives the reports and what action(s) they must take.
4. True or **false**: A Workflow can be either activated and scheduled to run, or it can be run once now, but not both.
5. Which button takes you to a particular item in your To Do list?
    i. GOTO
    ii. **VIEW**
    iii. OPEN
    iv. SAVE

Additional information

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Unit summary

Having completed this unit, you should be able to:

- Understand how to consolidate and automate audit activities into a compliance workflow
- Determine who needs to review the audit results and manage the signoffs
- Establish a schedule for delivery

© Copyright IBM Corporation 2011, 2013

Figure 12-17. Unit summary GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Exercise

- At this point, you should complete **Exercise 13** in the Exercise Guide.

© Copyright IBM Corporation 2011, 2013

Figure 12-18. Exercise GU2022.0

Notes:

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Checkpoint solutions

1. The three elements of a Compliance Automation Workflow process are a **distribution plan**, a **set of tasks**, and a **schedule**.
2. **True** or false: A user can optionally be notified of pending work in the Compliance Automation Workflow through a To Do list link.
3. The **receiver** table controls who receives the reports and what action(s) they must take.
4. True or **false**: A Workflow can be either activated and scheduled to run, or it can be run once now, but not both.
5. Which button takes you to a particular item in your To Do list?
    1. GOTO
    2. **VIEW**
    3. OPEN
    4. SAVE

© Copyright IBM Corporation 2011, 2013

Figure 12-19. Checkpoint solutions GU2022.0

Notes:

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Appendix A. Monitoring Overview

A.1. Introduction

This document describes the steps required to successfully implement database monitoring using the Guardium solution. In this context, we define monitoring as the review of database activity that can pose compliance or security violations. The end result of these steps is a process that automatically delivers your required reports to the appropriate staff members on a scheduled basis using Guardium's workflow automation.

The required steps include:

1. Gathering requirements
2. Building Groups
3. Defining Policy
4. Creating reports
5. Adding Guardium users and roles
6. Creating a workflow

The following sections explain these steps in detail.

A.2. Intended Audience

This document is intended to be used with customers who have some familiarity with the Guardium solution and, preferably, are currently working on an implementation with a Professional Services consultant.

A.3. Gathering Requirements

The first step is to define your requirements. Requirements are often determined by an organization's auditors, especially in SOX or PCI implementation, but can also be determined by internal security rules.

If you do not have a clear definition of your requirements, try to answer the following questions:

Logging and real-time alerting:

- **Who** needs to be monitored? Privileged users, DBAs, everyone?
- What types of **actions** must be monitored? DDL, DML, selects on specific tables?
- What type of information can safely be **ignored**?
- What type of activity should prompt **alerts**?
- What type of activity should prompt more **verbose** logging (that is, logging the full SQL string, including values)?
- What are your **sensitive** objects?

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Reporting:

- What **reports** do I need?
- What **fields** do I need in my reports?
- What should prompt an action to appear on my reports (query **conditions**)?

Audit Review:

- **Who** needs to receive monitoring reports?
- How **frequently** should reports be delivered?
- Should users be required to **sign** reports or is reviewing reports sufficient (sign off of reports can be configured on a per user basis)?
- Should the delivery of reports stop at any receivers until they have reviewed or signed off on them or should they be delivered to all users at once?

Requirements Example

Below are examples of some common monitoring requirements. We will use these examples throughout the document to show how your requirements can be met using Guardium's toolset.

- Report on DDL activity in production
- Report on all activity by privileged users including the Full SQL string
- Report on DML on Sensitive Objects, including the Full SQL string
- Alert on three or more failed logins by the same user within five minutes
- Alert on DML against Sensitive Objects
- Ignore activity by applications, backup jobs, and other scheduled processes
- Reports should be delivered to Information Security (IS) group and signed by the IS manager. After the IS Manager has signed the reports, the reports should be delivered to the Audit and Database Manager groups for review
- Delivery of reports should be broken down by database type: MS SQL Server or Oracle

A.4. Building Groups

Groups simplify policy and query creation by allowing users to organize Guardium data elements based on their reporting requirements. It is much easier to create your reports and policy after you have defined your groups. For example, assume that your company has 25 separate data objects containing sensitive employee information, and you need to report on all access to these items. You could formulate a very long query testing for each of the 25 items. Alternatively, you could define a single group called sensitive objects, containing those 25 objects. That way, in queries or policy rule definitions, you only need include the group in the where clause, instead of each, separate, object.

There are six ways to populate groups. Generally, manual entry is sufficient but if you need to load a large number of members, or want to update a group on a scheduled basis, one of the other methods might be more appropriate.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Methods to Populate Groups:

1. Manual Entry.
2. **LDAP:** Imports group members from you LDAP or Active Directory Servers.
3. **Populate from Query:** Adds group members based on data in Guardium's database (this data can be imported from an external data source).
4. **Auto Generated Calling Prox:** Analyzes stored procedures and updates an object group based on the what the procedure does or the data it accesses.
5. **Classification:** Analyzes databases and updates groups based on patterns in the data (for example, it can search for text patterns in tables that could contain credit card numbers and then add the tables to a sensitive object group).
6. **Guard:** Allows you to import a large number of group members from a flat file via SSH.

Example Groups

Below are the necessary groups based the example requirements from Step 1:

REQUIREMENT	GROUP
All DDL activity in production	**Name** = DDL Commands **Type** = Commands **Members** = Built in group with over 70 members **Name** = - Monitoring Productions Servers **Type** = Server IP **Members** = 10.10.9.1, 10.10.9.80, 10.10.9.173
Ignore activity by backup and other scheduled processes	**Name** = - Monitoring Scheduled Processes **Type** = Source Programs **Members** = RMAN, MSBackup, SQSH
Log full details by privileged users	**Name** = - Monitoring Privileged Users **Type** = Users **Members** = sa, sys, system, a4920, a2840, a9404, a8000, a4939
Alert on three or more failed logins within five minutes	n/a
Log full details and alert on DML against Sensitive Objects	**Name** = DML Commands **Type** = Commands **Members** = Built in group with 8 members **Name** = - Monitoring Sensitive Objects **Type** = Objects **Members** = scott.cc_numbers, scott.ssn_numbers, customers, employees, addresses

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

A.5. Defining Policy

A policy is a set of rules and actions that are applied against SQL traffic as it is captured by the Guardium appliance in real time. Each rule within the policy contains a set of criteria and one action. For example, send an alert via e-mail any time DML is executed against a sensitive object. Each rule is applied in sequence as the data is being collected in real time.

This is where we ensure that activity is logged based on your monitoring requirements as defined by the Logging and real-time alerting questions from step one. Policies define what traffic should be ignored, what activities require more detail, and which actions should prompt real-time alerts.

The order and logic of the policy is very important. Also, there are options that can completely change the methods used to log data. These methods include Selective Audit Trail, Flat Logging and Baselines. Please refer to the user manual or ask your Professional Services Consultant for further details on these options.

Example Policy based on the example requirements from Step 1. If a requirement is not listed here, it means that no special policy action is required. By default all data is logged without values.

Rule #	Rule Type	Requirement	Rule Description	Criteria	Action	Continue to next Rule
1	Exception	Alert on three or more failed logins within five minutes	Failed Logins - Alert on 3 Failed Logins in 5 minutes	Exception Type = LOGIN_FAILED Min. Ct = 3 Reset Interval = 5	ALERT PER MATCH	No
2	Access	Ignore activity by applications, backup jobs, and other scheduled processes	Scheduled Processes - Ignore Session	Source Program Group = - Monitoring Scheduled Processes	IGNORE STAP SESSION*	No
3	Access	Report on all activity by privileged users including the Full SQL string	Privileged Users - Log Full Details	DB User Group = - Monitoring Privileged Users	LOG FULL DETAILS*	Yes
4	Access	Alert on DML against Sensitive Objects	DML on Sensitive Objects - Alert	Object Group = - Monitoring Sensitive Objects Command Group = DML Commands	ALERT PER MATCH	Yes
5	Access	Report on DML against Sensitive Objects, including the Full SQL string	DML on Sensitive Objects - Log Full Details	Object Group = - Monitoring Sensitive Objects Command Group = DML Commands	LOG FULL DETAILS	No

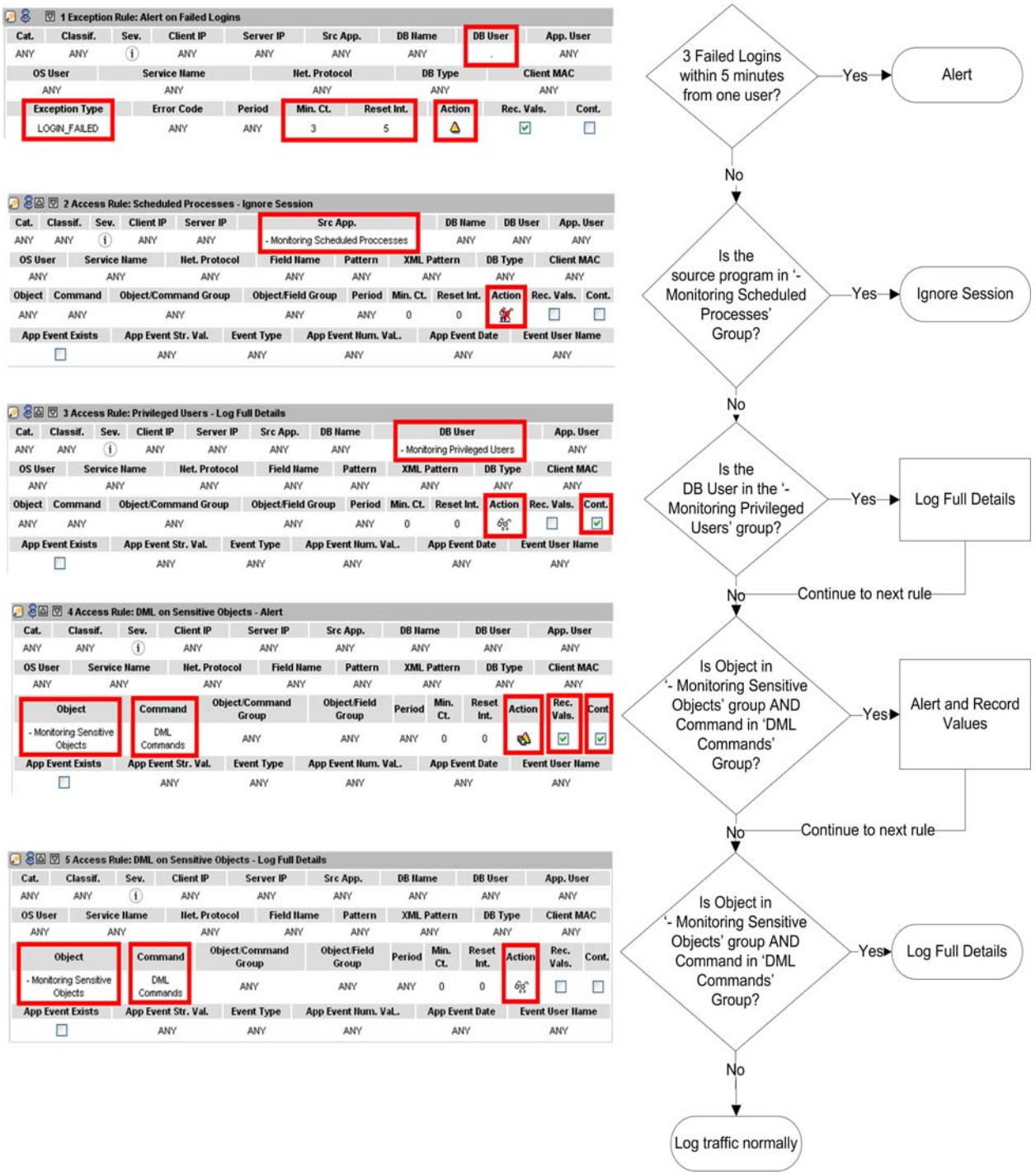
© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

* The appendix at the end of this document provides additional definitions of the 'Ignore STAP Session' and 'Log Full Details' rules.

The flow chart on the next page demonstrates how commands are processed by the policy rules.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.


1 Exception Rule: Alert on Failed Logins
Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User
ANY ANY ANY ANY ANY ANY
OS User Service Name Net. Protocol DB Type Client MAC
ANY ANY ANY ANY ANY
Exception Type Error Code Period Min. Ct. Reset Int. Action Rec. Vals. Cont.
LOGIN_FAILED ANY ANY 3 5
2 Access Rule: Scheduled Processes - Ignore Session
Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User
ANY ANY ANY ANY - Monitoring Scheduled Proccesses ANY ANY ANY
OS User Service Name Net. Protocol Field Name Pattern XML Pattern DB Type Client MAC
ANY ANY ANY ANY ANY ANY ANY ANY
Object Command Object/Command Group Object/Field Group Period Min. Ct. Reset Int. Action Rec. Vals. Cont.
ANY ANY ANY ANY ANY 0 0
App Event Exists App Event Str. Val. Event Type App Event Num. Val.. App Event Date Event User Name
ANY ANY ANY ANY ANY
3 Access Rule: Privileged Users - Log Full Details
Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User
ANY ANY ANY ANY ANY ANY - Monitoring Privileged Users ANY
OS User Service Name Net. Protocol Field Name Pattern XML Pattern DB Type Client MAC
ANY ANY ANY ANY ANY ANY ANY ANY
Object Command Object/Command Group Object/Field Group Period Min. Ct. Reset Int. Action Rec. Vals. Cont.
ANY ANY ANY ANY ANY 0 0
App Event Exists App Event Str. Val. Event Type App Event Num. Val.. App Event Date Event User Name
ANY ANY ANY ANY ANY
4 Access Rule: DML on Sensitive Objects - Alert
Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User
ANY ANY ANY ANY ANY ANY ANY ANY
OS User Service Name Net. Protocol Field Name Pattern XML Pattern DB Type Client MAC
ANY ANY ANY ANY ANY ANY ANY ANY
Object Command Object/Command Group Object/Field Group Period Min. Ct. Reset Int. Action Rec. Vals. Cont
- Monitoring Sensitive Objects DML Commands ANY ANY ANY 0 0
App Event Exists App Event Str. Val. Event Type App Event Num. Val.. App Event Date Event User Name
ANY ANY ANY ANY ANY
5 Access Rule: DML on Sensitive Objects - Log Full Details
Cat. Classif. Sev. Client IP Server IP Src App. DB Name DB User App. User
ANY ANY ANY ANY ANY ANY ANY ANY
OS User Service Name Net. Protocol Field Name Pattern XML Pattern DB Type Client MAC
ANY ANY ANY ANY ANY ANY ANY ANY
Object Command Object/Command Group Object/Field Group Period Min. Ct. Reset Int. Action Rec. Vals. Cont.
- Monitoring Sensitive Objects DML Commands ANY ANY ANY 0 0
App Event Exists App Event Str. Val. Event Type App Event Num. Val.. App Event Date Event User Name
ANY ANY ANY ANY ANY
3 Failed Logins within 5 minutes from one user?
Yes
Alert
No
Is the source program in '- Monitoring Scheduled Processes' Group?
Yes
Ignore Session
No
Is the DB User in the '- Monitoring Privileged Users' group?
Yes
Log Full Details
No
Continue to next rule
Is Object in '- Monitoring Sensitive Objects' group AND Command in 'DML Commands' Group?
Yes
Alert and Record Values
No
Continue to next rule
Is Object in '- Monitoring Sensitive Objects' group AND Command in 'DML Commands' Group?
Yes
Log Full Details
No
Log traffic normally

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

A.6. Creating Reports

Now that the groups and policies have been defined, we are ready to create our queries and reports. These are required elements in creating your queries/reports:

1. **Main Entity**

The main entity defines the data type that will be the main focus of the report. Generally, you will choose one of the following four main entities:

- **Session:** Used when reporting on successful logins to the database server. This main entity provides one line per login, with no detail on the activity performed by the user.
- **Command:** Used when user actions are the main focus of the report. Each individual command that a user issues will have its own line on the report.
- **Object:** Used if the actual object name accessed is required. Each object accessed will appear on separate line. Generally, this will result in multiple lines per SQL requests (one for each object referenced in the SQL requests).
- **SQL (or Full SQL if logging full details):** Used to provide one line per unique SQL statement. This is appropriate if you require the SQL statement in your report.

Note

A complete SQL statement can be hundreds of lines long and can make reports very difficult to read.

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

2. **Query Attributes**

Query Attributes are the fields that will appear in the report. The most commonly used attributes include:

- Time Stamp
  - From Access Period if using Command or Object main entity and you are not logging full details
  - From Full SQL if you are logging full details
- Session Start
- Client/Server: Server IP
- Client/Server: Client IP
- Client/Server: DB User Name
- Client/Server: Source Program
- Session: Database Name
  - (Client/Server: Service Name if Oracle)
- Command: SQL Verb (If using a Main Entity of Command or lower)
- Object: Object Name (if using a Main Entity of Object or lower)
- SQL: SQL (or Full SQL if logging full details): Some customers do choose to include the SQL statement in the report, which works well if only small SQL statements are issued. However, many SQL statements can be hundreds of lines and can cause the report to become very difficult to read.

3. **Query conditions**

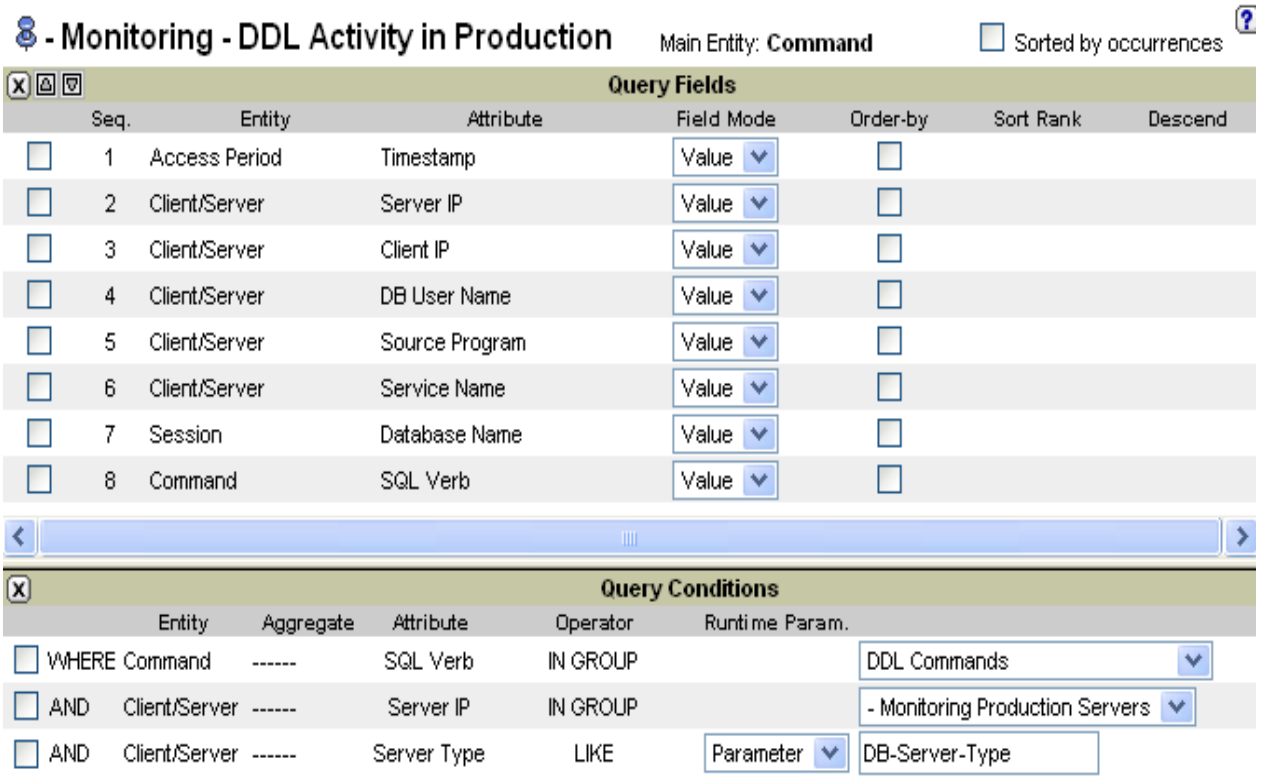
The query conditions filter the data that will appear on your reports (the where clause of your query). Because we have defined our groups in Step 2, creating the Where clause is very simple.

As a best practice, try to use Groups or Run-time Parameters, instead of hard coding values, whenever possible. This allows for much more flexibility later, if you need to change your reports. Run-time parameters also allow you to produce multiple result sets from a single query.

Below are the fields and conditions for the first report in the requirements list: *Report on DDL activity in production*.

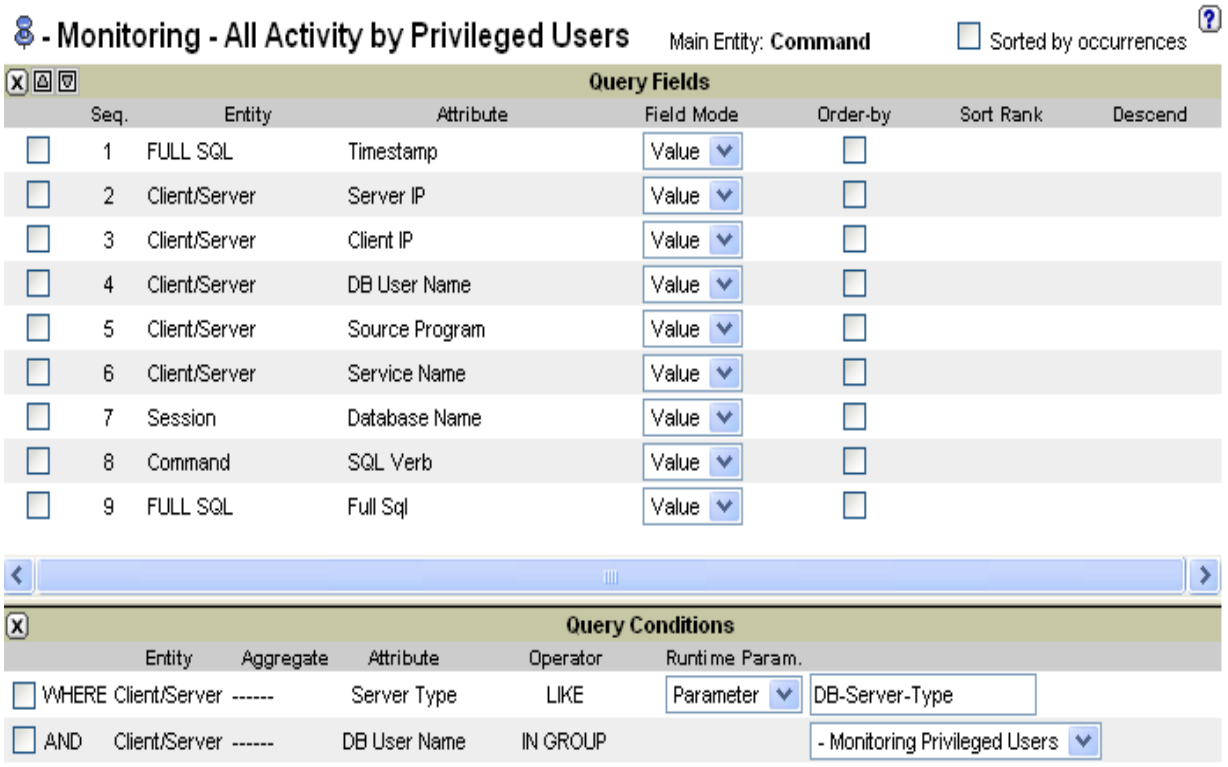
 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.


- Monitoring - DDL Activity in Production
Main Entity: Command
Sorted by occurrences
Query Fields
Seq. Entity Attribute Field Mode Order-by Sort Rank Descend
1 Access Period Timestamp Value
2 Client/Server Server IP Value
3 Client/Server Client IP Value
4 Client/Server DB User Name Value
5 Client/Server Source Program Value
6 Client/Server Service Name Value
7 Session Database Name Value
8 Command SQL Verb Value
Query Conditions
Entity Aggregate Attribute Operator Runtime Param.
WHERE Command ------ SQL Verb IN GROUP DDL Commands
AND Client/Server ------ Server IP IN GROUP - Monitoring Production Servers
AND Client/Server ------ Server Type LIKE Parameter DB-Server-Type

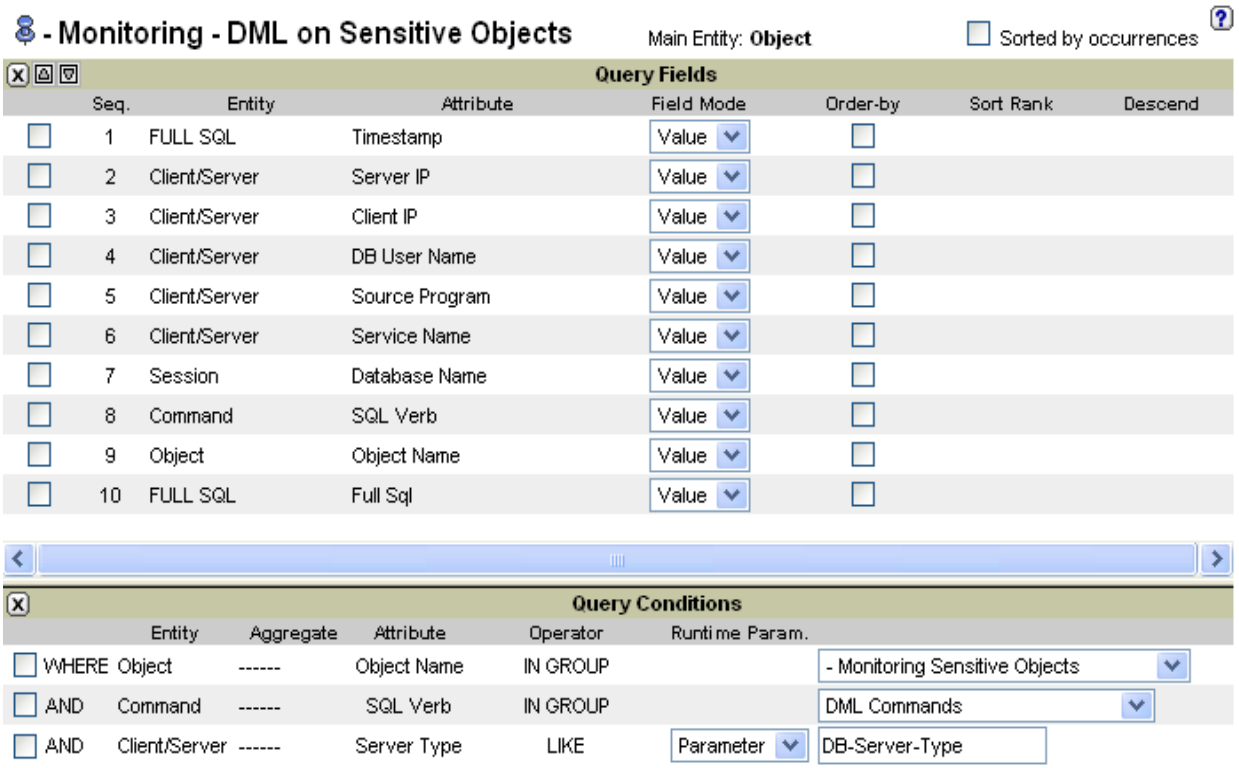
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

The second reporting requirement, *Report on all activity by privileged users including the Full SQL string*, will have slightly different attributes because the *Full SQL String* is requested. Also, logging full details, allows us to use the Full SQL Timestamp, which is more precise than the Access Period Timestamp.


- Monitoring - All Activity by Privileged Users
Main Entity: Command
Sorted by occurrences
Query Fields
Seq. Entity Attribute Field Mode Order-by Sort Rank Descend
1 FULL SQL Timestamp Value
2 Client/Server Server IP Value
3 Client/Server Client IP Value
4 Client/Server DB User Name Value
5 Client/Server Source Program Value
6 Client/Server Service Name Value
7 Session Database Name Value
8 Command SQL Verb Value
9 FULL SQL Full Sql Value
Query Conditions
Entity Aggregate Attribute Operator Runtime Param.
WHERE Client/Server ------ Server Type LIKE Parameter DB-Server-Type
AND Client/Server ------ DB User Name IN GROUP - Monitoring Privileged Users

The final reporting requirement, *Report on DML on Sensitive Objects, including the Full SQL string*, is similar to the second but must be created with **Object** as the main entity because the user is interested in *Sensitive Objects*.

© Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.



- Monitoring - DML on Sensitive Objects

Main Entity: **Object**

Sorted by occurrences

Query Fields

	Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
☐	1	FULL SQL	Timestamp	Value	☐		
☐	2	Client/Server	Server IP	Value	☐		
☐	3	Client/Server	Client IP	Value	☐		
☐	4	Client/Server	DB User Name	Value	☐		
☐	5	Client/Server	Source Program	Value	☐		
☐	6	Client/Server	Service Name	Value	☐		
☐	7	Session	Database Name	Value	☐		
☐	8	Command	SQL Verb	Value	☐		
☐	9	Object	Object Name	Value	☐		
☐	10	FULL SQL	Full Sql	Value	☐		

Query Conditions

		Entity	Aggregate	Attribute	Operator	Runtime Param.	
☐	WHERE	Object	------	Object Name	IN GROUP		- Monitoring Sensitive Objects
☐	AND	Command	------	SQL Verb	IN GROUP		DML Commands
☐	AND	Client/Server	------	Server Type	LIKE	Parameter	DB-Server-Type

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

A.7. Adding Guardium Users and Roles

Now that you have created all of your required reports, Guardium's workflow functionality allows you to automatically deliver them to end users. To enable your users to receive workflow automation results, however, they must be added within Guardium first.

Workflow results can be delivered to users or roles (a group of one or more users). As a best practice, workflow results should be delivered to roles. This allows more than one user to sign-off on a result set and is easier to manage employee turnover.

Below are the required steps to create users and roles within Guardium.

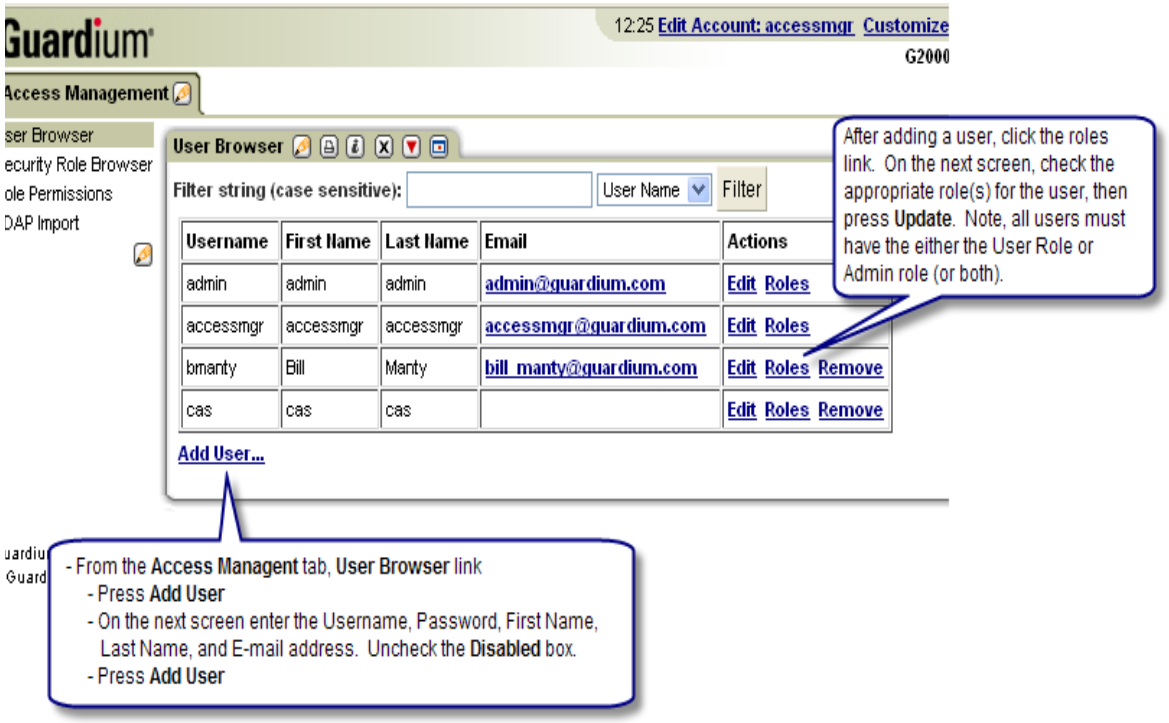
1. Define your roles by answering the following questions.
   a. Who should receive reports and what are the job functions of each receiver (Audit, Information Security DBA Manager, and so on).
   b. What users have the same job functions and can provide an equivalent sign off? (that is, Bob and Jane are both Information Security Officers. Bob will primarily sign off on Guardium reports but Jane should be able to so as well, in Bob's absence).

Each job function should be added as a role and each receiver as a Guardium user. The users should be added to the appropriate role based on their job function.

2. Create your roles as shown below. (This must be performed by a user with the accessmgr role.)

 © Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

3. Create your users and assign the appropriate role. (This must be performed by a user with the accessmgr role.)



Based on our example requirement below are the necessary groups and users.

Example Roles and Users (Requirement: Reports should be delivered to Information Security (IS) group and signed by the IS manager. After the IS Manager has signed the reports, the reports should be delivered to the Audit and Database Manager groups for review

ROLE	USERS
Information Security	Jim McNulty (jmcnulty), Jay Landsman (jlandsman), Lester Freamon (lfreamon), Russell Bell (rbell)
Information Security Manager	Russell Bell (rbell)
Audit	Joe Stewart (jstewart), Ellis Carver (ecarver), Thomas Hauk (thauk)
Database Manager	Bill Rawls (brawls), Omar Little (olittle)

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

A.8. Developing Workflow

Now that we have defined our reports, users, and roles we must create an Audit Process to deliver the reports to the appropriate users based on our requirements.

The Audit Process Builder is used to define:

- **Who** receives the reports
- Which **reports** are delivered
- The **frequency** of delivery
- The **workflow**, which includes
  - The order of delivery
  - Whether sign-off is required
  - Whether the delivery should stop at any user or role until they have reviewed or signed off on the audit process

Based on our Requirements, below is an example of how to configure an audit process:

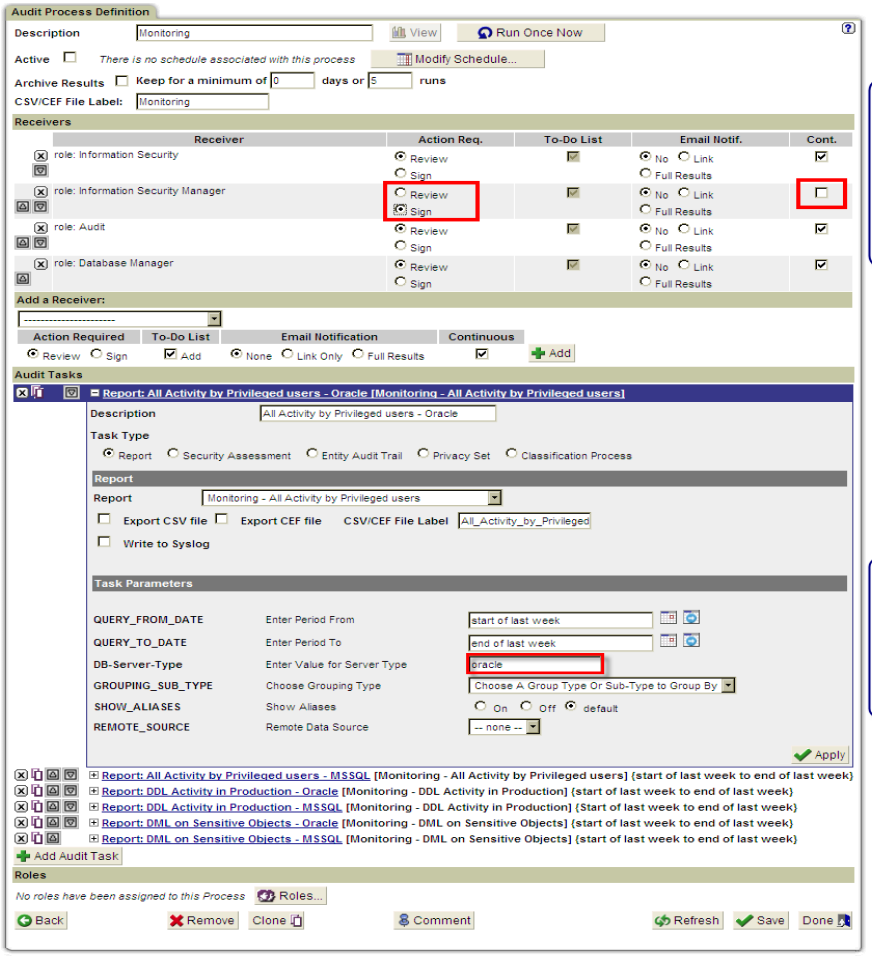
Example Requirements

- Reports should be delivered to Information Security (IS) group and signed by the IS manager. After the IS Manager has signed the reports, the reports should be delivered to the Audit and Database Manager groups for review
- Delivery of reports should be broken down by database type: MS SQL Server or Oracle

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

Example Audit Process



Under **Receivers**, enter each role based on the order in the requirements. Because the Audit and Database Manager roles, should not receive the audit process until the Information Security Manager has signed them, **Action Req.** is marked as *Sign* for the Information Security Manager role. Also, the **Cont.** checkbox is unchecked, so that it will not reach subsequent users until it has been signed.

Next, enter all of the reports to be delivered as displayed here. Since, the requiement is that Oracle and MS SQL traffic should be in separate reports, create each task twice, using the DB-Server-Type runtime parameter, to breakout each database type.

Repeat this step for each report.

After entering all the receivers and audit tasks, mark the audit process as active and press Modify Schedule to schedule delivery of the audit process.

© Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

A.9. Appendix

9.1 Policy Definitions

Ignore STAP Session

Ignore STAP Session causes the collector to send a signal STAP instructing it to stop sending all traffic, except for the logout notification, for specific sessions.

For example, if you have a rule that says 'where DBUserName?=scott, Ignore STAP Session':

- When Scott logs into the database server, STAP sends the connection information to the collector.
- The collector logs the connection. Session information (log in/log outs) are always logged.
- The collector sends a signal to STAP to stop sending any more traffic from this specific session. This means that any commands run by Scott against the database server and any responses (result sets, SQL errors, and so on) sent by the Database server to Scott will be discarded by STAP and will never reach the collector.
- When Scott logs out of the database server, STAP will send this information to the collector (log in/log out information is always tracked even if the session is ignored).
- When Scott logs in again, the steps above are repeated. The logic on which sessions should be ignored is maintained by the collector, not STAP.

Log Full Details

By default the Guardium collector will mask all values when logging a SQL string. For example 'insert into tableA (name,ssn,ccn) values ('Bob Jones', '429-29-2921','29249449494949494')' will be logged as 'insert into tableA (name,ssn,ccn) values (?, ?,?)'. This is the default behavior for two reasons.

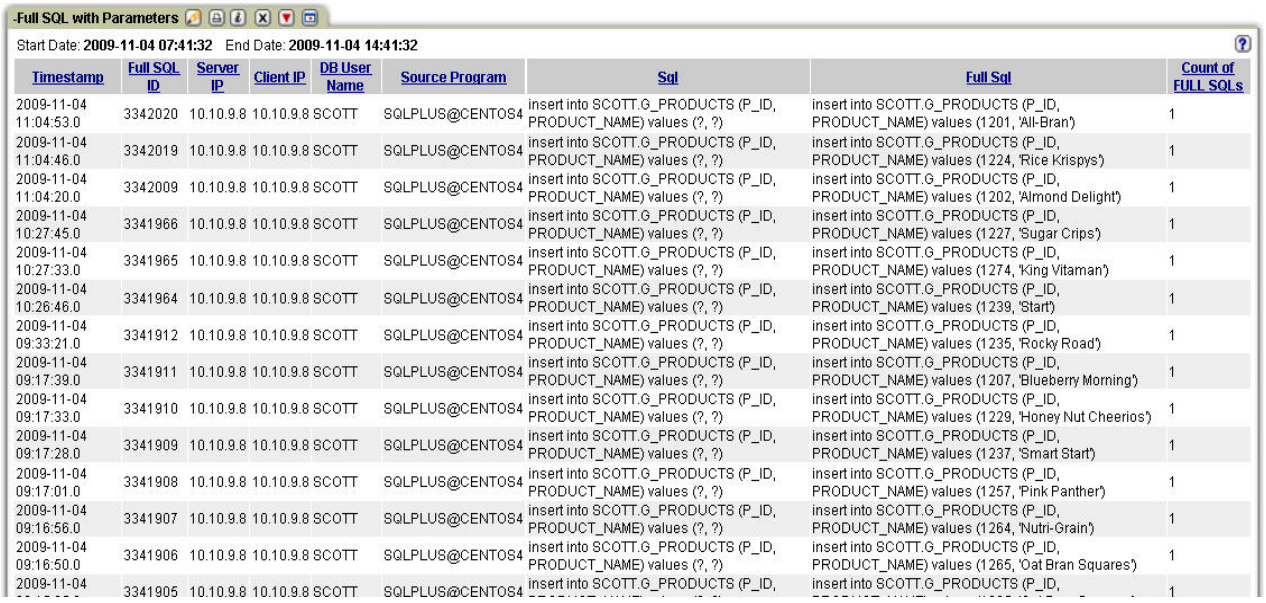
1. Values should not be logged by default because they might contain sensitive information.
2. Logging without values can provide for increased system performance and longer data retention within the appliance. Very often, database traffic consists of many SQL requests, identical in everything except for their values, repeated hundreds, thousands, or even millions of times per hour. By masking the values, Guardium is able to aggregate these repeated SQL requests into a single request, called a *construct*. When constructs are logged, instead of each individual SQL request/construct being logged separately, it is only logged once per hour (per session) with a counter of how many times the construct was executed. This can save a tremendous amount of disk space because, instead of creating a hundreds (or millions) of lines in the database, only one new line is added.

 © Copyright IBM Corp. 2011, 2013

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

-SQL
Start Date: 2009-11-04 07:41:32 End Date: 2009-11-04 14:41:32
Session Id | Timestamp | Server IP | Client IP | DB User Name | Source Program | Sql | Total access
548588 | 2009-11-04 09:13:13.0 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | 94
548594 | 2009-11-04 09:32:29.0 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | 11
548594 | 2009-11-04 10:26:53.0 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | 3
548594 | 2009-11-04 11:04:10.0 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | 3
Records: 1 to 4 of 4
When logging constructs without values the constructs are logged are logged once per hour per session. Instead of adding addtional lines per SQL Request, the Total Access is incremented and the timestamp is updated. So, in this example, the system logged four additional lines instead of 111.

When logging with *Full Details*, in addition to logging the data as shown above, Guardium logs the data with the values unmasked and each separate request as shown below. Logging Full Details also provides the exact timestamp whereas logging without details provides the most recent timestamp of a construct within the logging granularity time period (usually 1 hour).


-Full SQL with Parameters
Start Date: 2009-11-04 07:41:32 End Date: 2009-11-04 14:41:32
Timestamp | Full SQL ID | Server IP | Client IP | DB User Name | Source Program | Sql | Full Sql | Count of FULL SQLs
2009-11-04 11:04:53.0 | 3342020 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1201, 'All-Bran') | 1
2009-11-04 11:04:46.0 | 3342019 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1224, 'Rice Krispys') | 1
2009-11-04 11:04:20.0 | 3342009 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1202, 'Almond Delight') | 1
2009-11-04 10:27:45.0 | 3341966 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1227, 'Sugar Crips') | 1
2009-11-04 10:27:33.0 | 3341965 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1274, 'King Vitaman') | 1
2009-11-04 10:26:46.0 | 3341964 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1239, 'Start') | 1
2009-11-04 09:33:21.0 | 3341912 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1235, 'Rocky Road') | 1
2009-11-04 09:17:39.0 | 3341911 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1207, 'Blueberry Morning') | 1
2009-11-04 09:17:33.0 | 3341910 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1229, 'Honey Nut Cheerios') | 1
2009-11-04 09:17:28.0 | 3341909 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1237, 'Smart Start') | 1
2009-11-04 09:17:01.0 | 3341908 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1257, 'Pink Panther') | 1
2009-11-04 09:16:56.0 | 3341907 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1264, 'Nutri-Grain') | 1
2009-11-04 09:16:50.0 | 3341906 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (?, ?) | insert into SCOTT.G_PRODUCTS (P_ID, PRODUCT_NAME) values (1265, 'Oat Bran Squares') | 1
2009-11-04 | 3341905 | 10.10.9.8 | 10.10.9.8 | SCOTT | SQLPLUS@CENTOS4 | insert into SCOTT.G_PRODUCTS (P_ID,

Log Full Details with Values

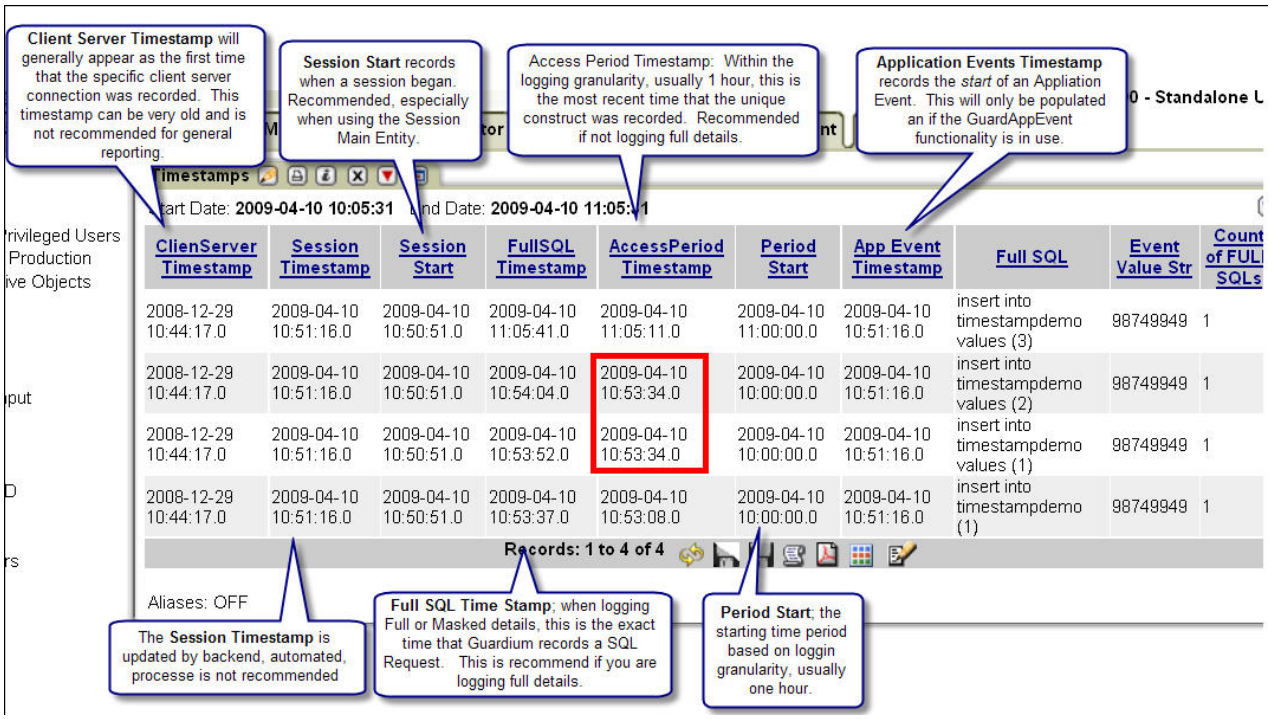
In a policy rule, you will see options for *Log Full Details* and *Log Full Details with Values*. *Log Full Details* provides the Full SQL string and exact timestamp as shown above. *Log Full Details with Values* will do the same and will also parse and log the values into a

Course materials may not be reproduced in whole or in part
without the prior written permission of IBM.

separate table in the database. This creates a great deal of additional overhead and is recommended that you discuss this with Guardium Services, if you think you need this option. *Log Full Details* is generally sufficient for most reporting needs.

9.2 Timestamps

The illustration below describes the different timestamp options available in the Query Builder.


Client Server Timestamp will generally appear as the first time that the specific client server connection was recorded. This timestamp can be very old and is not recommended for general reporting.
Session Start records when a session began. Recommended, especially when using the Session Main Entity.
Access Period Timestamp: Within the logging granularity, usually 1 hour, this is the most recent time that the unique construct was recorded. Recommended if not logging full details.
Application Events Timestamp records the start of an Appliation Event. This will only be populated an if the GuardAppEvent functionality is in use.
Timestamps
Start Date: 2009-04-10 10:05:31
End Date: 2009-04-10 11:05:11
ClienServer Timestamp
Session Timestamp
Session Start
FullSQL Timestamp
AccessPeriod Timestamp
Period Start
App Event Timestamp
Full SQL
Event Value Str
2008-12-29 10:44:17.0
2009-04-10 10:51:16.0
2009-04-10 10:50:51.0
2009-04-10 11:05:41.0
2009-04-10 11:05:11.0
2009-04-10 11:00:00.0
2009-04-10 10:51:16.0
insert into timestampdemo values (3)
98749949
1
2009-04-10 10:53:34.0
2009-04-10 10:54:04.0
2009-04-10 10:53:52.0
2009-04-10 10:53:37.0
2009-04-10 10:53:08.0
insert into timestampdemo values (2)
insert into timestampdemo values (1)
insert into timestampdemo (1)
Records: 1 to 4 of 4
Aliases: OFF
The Session Timestamp is updated by backend, automated, processe is not recommended
Full SQL Time Stamp; when logging Full or Masked details, this is the exact time that Guardium records a SQL Request. This is recommend if you are logging full details.
Period Start; the starting time period based on loggin granularity, usually one hour.

 © Copyright IBM Corp. 2011, 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.